



Onderzoek voor het WODC

Internationale verkenning bevoegdheden online gegevensvergaring politie bij (dreigende) openbare ordeverstoringen

Groningen, oktober 2025

www.pro-facto.nl

Colofon

Pro Facto
Ossenmarkt 5
9712 NZ Groningen
www.profacto.nl
info@profacto.nl
050-3139853

Auteurs	Heinrich Winter, Christian Boxum, Jeanne Cazemier, Thijs Drouen en Stef Roest
Opdrachtgever	WODC
Datum	Oktober 2025
Status	Definitief

Dit onderzoek is – in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum – uitgevoerd door Pro Facto, bureau voor bestuurskundig en juridisch onderzoek, advies en onderwijs.

Begeleidingscommissie:

Prof. mr. Jon Schilder (Vrije Universiteit), mr. Bart Engberts (J&V), dr. Bart van der Sloot (Tilburg University), mr. Hester van der Sluis (J&V), drs. Frank Willemsen (WODC).

Voor de inhoud van het rapport zijn de onderzoekers verantwoordelijk. Het leveren van een bijdrage (als medewerker van een organisatie of als lid van de begeleidingscommissie) betekent niet automatisch dat de betrokkene instemt met de gehele inhoud van het rapport. Dat geldt eveneens voor het ministerie van Justitie en Veiligheid en zijn minister.

© 2025 Pro Facto. Auteursrechten voorbehouden.

Inhoud

Samenvatting	5
1. Inleiding	12
1.1 Aanleiding	12
1.2 Pleidooien voor verduidelijking en verruiming van online politiebevoegdheden	13
1.3 Regelingen in het buitenland	14
1.4 Centrale onderzoeksvragen	14
1.5 Opzet van het onderzoek	14
1.6 Onderzoeksaanpak en -verantwoording	15
1.6.1 Oriënterende fase	15
1.6.2 Deelonderzoek A – brede verkenning	15
1.6.3 Deelonderzoek B – verdieping	16
1.7 Conclusie dataverzameling	18
1.8 Leeswijzer	19
2. Frankrijk	20
2.1 Organisatie van de openbare ordehandhaving	20
2.2 Het wettelijk kader voor de uitoefening van de openbare ordetaak	21
2.3 De uitvoering van online informatievergaring	24
2.4 Toestemming voor en controle op informatievergaring	26
3. Engeland	33
3.1 Organisatie van de openbare ordehandhaving	33
3.2 Het wettelijk kader voor de uitoefening van de openbare ordetaak	34
3.1 De uitvoering van online informatievergaring	38
3.2 Toezicht	38
3.3 Inzet van technische hulpmiddelen	39
3.3.1 Toezicht op technische hulpmiddelen	39
4. Duitsland, deelstaat Hessen	40
4.1 Organisatie van de openbare ordehandhaving	40
4.2 Het wettelijk kader voor de uitoefening van de openbare ordetaak	41
4.3 De uitvoering van online informatievergaring	44
4.4 Toezicht	45
4.5 Inzet van technische hulpmiddelen	45
5. België	47

5.1	Organisatie van de openbare ordehandhaving	47
5.2	Het wettelijk kader voor de uitoefening van de openbare ordetaak	48
5.2.1	Mogelijkheden voor het doen van online onderzoek in België	50
5.3	De uitvoering van online informatievergaring	52
5.4	Toezicht	53
5.5	Inzet van technische hulpmiddelen	54
6.	Ierland	58
6.1	Organisatie van de openbare ordehandhaving	58
6.2	Het wettelijk kader voor de uitoefening van de openbare ordetaak	58
6.3	De uitvoering van online informatievergaring	60
6.4	Inzet van technische hulpmiddelen	60
6.4.1	Toezicht op het gebruik van technische hulpmiddelen	61
7.	Denemarken	62
7.1	Organisatie van de openbare ordehandhaving	62
7.2	Het wettelijk kader voor de uitoefening van de openbare ordetaak	63
7.3	De uitvoering van online informatievergaring	64
7.4	Inzet van technische hulpmiddelen	65
7.4.1	Toezicht op technische hulpmiddelen	66
8.	Zweden	67
8.1	Organisatie van de openbare ordehandhaving	67
8.2	Het wettelijk kader voor de uitoefening van de openbare ordetaak	67
8.3	Uitvoering van online informatievergaring	69
8.4	Inzet van technische hulpmiddelen	69
8.4.1	Toezicht op het gebruik van technische hulpmiddelen	70
9.	Spanje	72
9.1	Organisatie van de openbare ordehandhaving	72
9.2	Het wettelijk kader voor de uitoefening van de openbare ordetaak	72
9.3	De uitvoering van online informatievergaring	73
9.4	Inzet van technische hulpmiddelen	73
10.	Conclusies	75
10.1	Bevindingen	75
10.1.1	Frankrijk en Engeland: één integraal wettelijk kader, één toezichthouder	75
10.1.2	Duitsland: bevoegdheden voor openbare ordetaken voornamelijk op deelstaatniveau, belangrijke rol voor rechterlijke toetsing	76
10.1.3	België: geen specifieke grondslag voor het doen van online onderzoek	77
10.2	Slotbeschouwing	78
Bijlage 1:	Geraadpleegde bronnen	80

Bijlage 2: Lijst van gesprekspartners

84

Samenvatting

Aanleiding

De politie ziet zich steeds vaker geconfronteerd met verstoringen van de openbare orde die online hun oorsprong vinden of daar worden versterkt. Oproepen tot geweld of tot rellen of acties tijdens evenementen worden in toenemende mate verspreid via sociale media en digitale platforms. Dit maakt dat de politie – naast onder andere informatievergaring in de offline wereld, fysieke surveillance en informatie van de wijkagent – ook bij de feitelijke handhaving van de openbare orde niet zonder online informatie kan.

Het huidige Nederlandse juridisch kader biedt hiervoor echter geen concrete grondslag. Artikel 3 Politiewet (PW), waarin de algemene politietaak is vastgelegd, staat slechts toe dat de politie in beperkte mate persoonsgegevens verwerkt. Voor diepgaand online onderzoek – waarbij al snel een meer dan geringe inbreuk op de persoonlijke levenssfeer ontstaat – ontbreekt een specifieke wettelijke basis. In de strafvorderlijke sfeer bestaan wel uitgewerkte bevoegdheden (onder gezag van de officier van justitie), maar bij de bestuurlijke ordetaak moet de politie telkens opnieuw afwegen of de inzet van online middelen proportioneel is en past binnen de beperkte ruimte die artikel 3 PW laat.

Dit leidt tot dilemma's: enerzijds is er het belang van grondrechtenbescherming (artikel 8 EVRM, artikel 7 EU-Handvest, artikel 10 Grondwet). Anderzijds rust op de politie en het bestuur een duidelijke maatschappelijke plicht om ordehandhaving effectief uit te voeren.

Pleidooien voor verduidelijking en verruiming

Meerdere onderzoeken bevestigen dat het huidige wettelijk stelsel onvoldoende aansluit bij de digitale realiteit. Naar aanleiding van de avondklokrellen werd door onderzoekers bepleit dat de politie en gemeenten meer bevoegdheden zouden moeten krijgen om tijdig te kunnen reageren op signalen van maatschappelijke onrust die zich online ontwikkelen. Ook de Commissie-Koops adviseerde om de inzet van internetonderzoek voor de openbare ordetaak expliciet wettelijk te regelen, met een grondslag voor het verzamelen van persoonsgegevens uit publiek toegankelijke bronnen.

De minister van Justitie en Veiligheid sloot zich daar in 2022 bij aan: de minister stelde dat de politie over voldoende mogelijkheden moet beschikken om online onderzoek te doen bij de handhaving van de openbare orde. Daarbij werd onderstreept dat eventuele verruiming van

bevoegdheden altijd moet plaatsvinden binnen de grenzen van legitimiteit, noodzakelijkheid, proportionaliteit en democratische controle.

Regelingen in het buitenland

Om de ontwikkeling van een Nederlands wetsvoorstel goed te kunnen onderbouwen, is verkend hoe andere Europese landen de openbare ordetaak en online bevoegdheden hebben ingericht. Hoewel in alle EU-lidstaten de Richtlijn 2016/680 (over gegevensbescherming bij opsporing en handhaving) is geïmplementeerd, bestaan er aanzienlijke nationale verschillen in de reikwijdte van bevoegdheden, de rolverdeling tussen politie en bestuur, en de inrichting van toezicht. Deze verkenning geeft enig inzicht in een aantal buitenlandse openbare orde-stelsels, juridische constructies en waarborgen en kan ter inspiratie dienen voor de Nederlandse praktijk.

Centrale onderzoeksvragen

Het onderzoek is opgezet rond drie hoofdvragen:

1. Hoe ziet in verschillende Europese landen het juridisch kader eruit voor het verzamelen van (online) gegevens ten behoeve van de openbare ordetaak?
2. Wat is bekend over de effectiviteit en rechtmatigheid van de uitvoering van die taak?
3. Welke elementen uit buitenlandse regelingen zijn aanbevelenswaardig voor toepassing in Nederland?

Opzet en aanpak van het onderzoek

Het onderzoek zou in drie fasen worden uitgevoerd:

- Deelonderzoek A: een brede verkenning
- Deelonderzoek B: verdieping
- Deelonderzoek C: mogelijke toepassing in Nederland

Deelonderzoek A

Voor deelonderzoek A hebben we een brede verkenning van de juridische kaders en de mogelijkheden voor online informatievergaring in acht landen uitgevoerd. Hierbij lag de nadruk op de beschrijving van wet- en regelgeving, de betrokken actoren en waar mogelijk ook de inzet van technische hulpmiddelen. Dit deelonderzoek is uiteindelijk uitgebreid, waarbij voor de meeste landen nog aanvullende interviews zijn gehouden om de informatie uit het deskresearch te kunnen duiden en valideren. In eerste instantie zijn zeven landen onderzocht op basis van deskresearch en interviews. In overleg met de begeleidingscommissie is Frankrijk hier later nog aan toegevoegd. Vier landen zijn nader verdiept: Frankrijk, Engeland, Duitsland (deelstaat Hessen) en België.

Deelonderzoek B en C

Deelonderzoek B zou een verdieping betreffen waarbij in zou worden gegaan op de effectiviteit van de stelsels in de praktijk. Dit deelonderzoek kon niet worden uitgevoerd omdat vanuit alle geselecteerde landen geen medewerking werd verleend vanuit de politiepraktijk. De informatie uit de onderzochte landen is daarom zoveel mogelijk nog aangevuld met interviews met respondenten uit de wetenschap in de betreffende landen. Omdat deelonderzoek B niet kon worden uitgevoerd, gold dit ook voor deelonderzoek C.

Benadrukt moet worden dat het rapport daarmee vooral een verkenning is: het geeft inzicht in de wettelijke kaders en in de manier waarop toezicht en waarborgen elders zijn ingericht, maar minder in de dagelijkse operationele praktijk, de mate waarin deze effectief is en in overeenstemming met het recht.

In onderstaande paragrafen wordt ingegaan op de belangrijkste bevindingen per bestudeerd land. Alleen de landen die nader zijn verdiept (Frankrijk, Engeland, Duitsland (deelstaat Hessen) en België) worden hier besproken.

Frankrijk

De Franse politiediensten bestaan uit de Police Nationale (DGPN), de Gendarmerie Nationale (GN) en de Police Municipale (gemeentepolitie). Zowel de politie als de gendarmerie zijn werkzaam in het hele land en beschikken over dezelfde bevoegdheden. De politie werkt meer in de grote steden en de buitenwijken, terwijl de gendarmerie meer op het platteland te werk gaat. De kleinere steden worden ofwel door de gendarmerie ofwel door de politie bediend. Parijs (en Marseille) kent ook nog een préfet de police. De préfet de police de Paris (kort préfet de police genoemd) is naast bepaalde administratieve functies ook belast met de veiligheid van personen en goederen op het grondgebied van de agglomeratie Parijs. De préfet de police is belast met voorkomen en bestrijden van criminaliteit en de handhaving van de openbare orde. DGPN en de Gendarmerie beschikken daarnaast over gespecialiseerde diensten die tijdens openbare ordeverstoringen kunnen worden ingezet.

De wet *LOI n° 2015-912 relative au renseignement* uit 2015 vormt boek VIII van de Code de la Sécurité, een bundeling van wetten die regels geven over de binnenlandse veiligheid. Boek VIII vormt Boek VIII van de CSI fungeert als de wettelijke basis voor inlichtingenactiviteiten in Frankrijk en is de grondslag voor gegevensvergaring voor alle diensten, dus ook voor de gendarmerie en de police nationale wanneer zij de openbare orde handhaven. In boek VIII zijn de doelen van inlichtingen, zoals nationale veiligheid, territoriale integriteit, en de strijd tegen terrorisme neergelegd en worden de technieken die inlichtingendiensten mogen gebruiken bij het verzamelen van inlichtingen beschreven. De wet kent geen expliciete bepaling die gaat over online onderzoek in publiek toegankelijk bronnen. In dit wetboek vastgelegd op welke wijze controle wordt uitgevoerd op gegevensverzameling door de inlichtingendiensten. De introductie van deze wet kan niet los worden gezien van de aanslagen in 2015, waaronder die op Charlie Hebdo.

Diensten die wettelijk bevoegd zijn op het gebied van het vergaren van inlichtingen kunnen gebruik maken van inlichtingentechnieken. Het inlichtingenwerk is in Frankrijk bij verschillende organisaties neergelegd en verdeeld in een 'eerste cirkel' en een 'tweede cirkel'. Inlichtingendiensten in de eerste cirkel hebben de meeste bevoegdheden als het gaat om het gebruik van inlichtingendiensten. Voor de diensten in de tweede cirkel geldt dat het vergaren van inlichtingen slechts een deel van het werk uitmaken en de opdracht van deze dienst verder strekt dan het vergaren van inlichtingen alleen.

De inzet van inlichtingentechnieken is onderworpen aan de voorafgaande toestemming van de premier in de vorm van een vergunning, afgegeven na advies van de Commission Nationale de Contrôle des Techniques de Renseignement (hierna: de CNCTR). Dit is een bestuurlijke toezichthoudende autoriteit die erop toe ziet dat de technieken voor het verzamelen van inlichtingen door de verschillende inlichtingendiensten op het nationale grondgebied worden toegepast in overeenstemming met de wet. De CNCTR opereert onafhankelijk van de regering en het parlement. De CNCTR heeft een adviserende taak richting de premier over het gebruik van

de in de wet genoemde inlichtingentechnieken. Deze advisering vindt plaats voorafgaand aan de vergunningverlening door de premier voor de inzet van betreffende inlichtingentechniek (advisering a priori). Daarnaast is de CNCTR ook bevoegd om het gebruik van inlichtingentechnieken achteraf te controleren (controle a posteriori). De CNCTR beoordeelt of de inzet van de inlichtingentechniek plaatsvindt uitsluitend in het kader van de taak die aan de inlichtingendienst is toegekend, of de inzet kan worden gerechtvaardigd en of de inbreuken die worden gepleegd op de eerbiediging van het privéleven in verhouding staan tot het doel waarvoor de inbreuk wordt gemaakt.

Engeland

In het Verenigd Koninkrijk is de verantwoordelijkheid voor de handhaving van de openbare orde verdeeld over verschillende instanties op verschillende niveaus, waaronder lokale, regionale en nationale autoriteiten. Engeland heeft op basis van *The Police Act 1996* een centraal politiestelsel met aan het hoofd *The National Crime Agency* en daaronder lokale politiekorpsen. Lokale politiekorpsen, onder leiding van een *Chief Constable*, zijn belast met het waarborgen van de openbare veiligheid op lokaal niveau. De Chief Constable is het hoogste bevelhebber van het politiekorps en heeft de verantwoordelijkheid voor de algemene en dagelijkse leiding van het politiekorps en de uitvoering van de politieactiviteiten binnen hun jurisdictie, waaronder het handhaven van de openbare orde, het voorkomen en opsporen van misdrijven en het waarborgen van de veiligheid binnen de toegewezen regio.

Naast de Chief Constable die verantwoordelijk is voor operationele aangelegenheden, houdt de *Police and Crime Commissioner (PCC)* namens de samenleving toezicht op het politiekorps. De PCC is een gekozen functionaris en heeft als doel de belangen van de gemeenschap te vertegenwoordigen en het politiebeleid te beïnvloeden. De relatie tussen de Chief Constable en de PCC vormt een belangrijk aspect van het Engelse politiestelsel. De burgemeester heeft in het Engelse bestel geen direct gezag over de operationele beslissingen van de politie.

In het Verenigd Koninkrijk vindt de openbare ordehandhaving plaats binnen het kader van verschillende wetten en regelgeving, zoals de *Public Order Act 1986*, de *Criminal Justice and Public Order Act van 1994* en de *Football Spectators Act 1989*. Verder is relevant de *Regulation of Investigatory Powers Act 2000* (RIPA), die onder meer de toestemming/autorisatie regelt voor het uitvoeren van surveillancetechnieken (covert surveillance) door overheidsinstanties. De bevoegdheid voor overheidsinstanties, waaronder de politie, om (online) informatie te vergaren is geregeld in de *Investigatory Powers Act 2016*.

Deze wetten geven regels over de surveillance mogelijkheden, maar kennen geen expliciete bepalingen die gaan over het gebruik van online gegevensvergaring. Wel is geregeld dat surveillance altijd noodzakelijk, proportioneel en in overeenstemming met de mensenrechten moeten zijn. Vanaf 2015 zijn er landelijke, maar later ook lokale richtlijnen ontwikkeld door de *National Open Source Intelligence Working Group* (en in 2019 herzien) die kaders en definities bieden voor het gebruik van *open sources* in het operationele politiewerk.

De Investigatory Powers Commissioner's Office (IPCO) is het onafhankelijke toezichthoudende orgaan in het Verenigd Koninkrijk dat toezicht houdt op het gebruik van onderzoeksbevoegdheden door politiediensten, inlichtingendiensten en andere overheidsinstanties. De IPCO werd opgericht in het kader van de Investigatory Powers Act 2016 (IPA). De IPCO staat onder leiding van de Investigatory Powers Commissioner, doorgaans een voormalige rechter van het High Court of Court of Appeal.

Voor het gebruik van de meest ingrijpende bevoegdheden – zoals het tappen van communicatie, hacken van apparaten (equipment interference) of bulk data-acquisitie – geldt dat een minister eerst toestemming moet geven op basis van noodzaak en proportionaliteit. Deze toestemming wordt pas rechtsgeldig na goedkeuring door een Judicial Commissioner van de IPCO. De Judicial Commissioners beoordelen onafhankelijk of de aanvraag voldoet aan wettelijke eisen. Zij kunnen toestemming geven of weigeren, en bij twijfel aanvullende informatie opvragen. Naast de voorafgaande toets voert de IPCO periodieke inspecties en audits uit bij politiediensten, inlichtingendiensten en andere bevoegde instanties.

Duitsland (Hessen)

Duitsland kent een federale staatsstructuur. De federale politie (Bundespolizei) en de inlichtingendienst (Bundesnachrichtendienst, BND) vallen onder het gezag van de federale overheid en opereren op basis van federale wetten, zoals de Bundespolizeigesetz en de Gesetz über das Bundeskriminalamt (BKAG). Tegelijkertijd hebben de zestien Länder elk hun eigen politieorganisaties en -wetten.

De dagelijkse handhaving van de openbare zijn vooral de deelstaatpolities verantwoordelijk. In Hessen is dit de Landespolizei Hessen. De bevoegdheid die de Landespolizei Hessen heeft om op het internet te surveilleren vloeit voort uit de algemene taakomschrijving in artikel 11 van het Hessisches Gesetz über die öffentliche Sicherheit und Ordnung, dat de politie toestaat alle noodzakelijke maatregelen te nemen om gevaar voor de openbare orde en veiligheid af te wenden. Deze bepaling is techniekneutraal en geldt dus ook voor digitale omgevingen. Daarnaast bieden de Duitse Grondwet (Grundgesetz) en de Bundesdatenschutzgesetz het bredere juridische kader: zij staan gegevensverwerking door de overheid toe, mits die een wettelijke basis heeft en voldoet aan de eisen van noodzakelijkheid, proportionaliteit en doelbinding.

Op grond van de genoemde regelingen mag de Landespolizei Hessen onder meer informatie van openbare en deels openbare bronnen op het internet verzamelen. Daarbij gaat het om het gebruik van informatie die vrij toegankelijk is op het internet, zoals sociale media posts, forums, en andere openbare digitale platforms. Voor het surveilleren in open bronnen heeft de Duitse politie geen afzonderlijke toestemming nodig. Wanneer het gaat om surveilleren in besloten groepen op het internet heeft de politie een gerechtelijk bevel nodig. Hierbij is het interessant om te benoemen dat er in Duitsland een discussie over de grens tussen openbare en niet openbare bronnen. Zo is het onduidelijk of een chat- of facebookgroepen moet worden gezien als open of gesloten wanneer de politie beschikt over een uitnodigingslink of is toegelaten tot een bepaalde niet openbare groep.

Het toezicht op de politie in Hessen is verdeeld over verschillende instanties. Er zijn binnen de politiediensten interne functionarissen voor gegevensbescherming, die toezien op de naleving van privacyregels. Daarnaast bestaan er externe toezichthouders op gegevensbescherming, zowel op federaal niveau (zoals de Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI) als op Länder-niveau (bijvoorbeeld de Hessische Beauftragte für Datenschutz und Informationsfreiheit).

In Hessen worden technische hulpmiddelen ingezet, zoals cameratoezicht en ANPR. Camera-toezicht in openbare ruimten vereist een wettelijke basis en moet proportioneel zijn; burgers moeten bovendien worden geïnformeerd via zichtbare aanduidingen. De inzet van ANPR-systemen is sinds 2018 beperkt na een uitspraak van het Bundesverfassungsgericht, dat strengere eisen stelde aan doelgerichtheid, locatie en gegevensbescherming.

België

In België is de burgemeester primair verantwoordelijk voor de lokale openbare orde. Voor het bewaren of herstellen van de openbare orde is de burgemeester onder meer de verantwoordelijke overheid inzake de *bestuurlijke politie* op het grondgebied van de gemeente. Er is in België weinig geregeld als het gaat om bevoegdheden voor het doen van online onderzoek door de politie bij het handhaven van de openbare orde. België kent geen wet op de openbare orde waarin bevoegdheden aan de politie zijn toegekend ter handhaving van de openbare orde.

De burgemeester en de bestuurlijke politie opereren op basis van de Nieuwe Gemeentewet en de Wet op het politieambt (Wpa), waarbij de Wpa een meer algemene basis biedt voor het verzamelen van persoonsgegevens door de politie. De Wpa voorziet echter niet in een specifieke grondslag voor het doen van online onderzoek. Een eerder voorstel tot uitbreiding van artikel 26 Wpa, waarin – kort gezegd – werd geprobeerd om duidelijkheid te scheppen over het online surveilleren op publiek toegankelijke plaatsen, werd uiteindelijk niet ingevoerd.

Ondanks dat artikel 26 Wpa niet is uitgebreid tot online onderzoek volgt volgens sommige auteurs uit het Agora-arrest van het Hof van Cassatie dat artikel 26 Wpa een grondslag biedt voor het betreden van online publiek toegankelijke plaatsen door de politie. Het gebruik van een alias kan daarbij onder voorwaarden behoren tot de normale wijze van het bezoeken van delen van het internet door de politie. Hierbij wordt opgemerkt dat het arrest is uitgesproken in de context van een strafzaak (behorend bij de gerechtelijke politie), waarbij het Wetboek van strafvordering de politiebevoegdheden regelt. Overigens zijn er ook auteurs kritischer over de stelling dat artikel 26 Wpa ook geldt voor online onderzoek in het kader van de openbare orde handhaving.

We hebben voor deelonderzoek A in België twee interviews gehouden. Beide gesprekspartners geven aan dat de bestuurlijke politie in België gebruik maakt van online onderzoek voor het handhaven van de openbare orde.

Het toezicht op de politie in België is verdeeld over verschillende instanties. Het toezicht bestaat uit intern toezicht binnen de politie, maar ook uit extern toezicht door toezichthouders als de Algemene inspectie, Comité P en Het Controleorgaan op de Politie-informatie.

In België worden verder bewakingscamera's en ANPR-systemen ingezet als technische hulpmiddelen. Regels voor de inzet en het gebruik van bewakingscamera's zijn vastgelegd in verschillende regelingen. Zo is er onder meer wetgeving in het gebruik van bijzondere opsporingsmethodes, voor bewakingscamera's in het algemeen en voor bewakingscamera's in voetbalstadions. Het gebruik van camera's door de politie wordt geregeld door de Wpa. Camera's van andere partijen zoals steden en gemeenten worden geregeld door de Camerawet.

1. Inleiding

1.1 Aanleiding

Criminaliteit speelt zich in toenemende mate online af. Oproepen tot geweld of het verstoren van de openbare orde worden steeds vaker gedeeld en aangejaagd op sociale media. Deze realiteit maakt dat de politie moet beschikken over online informatie om de politietaak goed te kunnen uitvoeren. Dit geldt voor zowel opsporing als handhaving van de openbare orde. Daarom gebruikt de politie online informatie, door de hele organisatie heen: van online specialisten tot en met de (digitale) wijkagent. In het huidige wettelijke bestel zijn de mogelijkheden van de politie om online informatie te verzamelen echter beperkt. De politie kan namelijk slechts onder strafvorderlijke titel en onder gezag van de officier van justitie, in het kader van opsporing van strafbare feiten, een meer dan geringe inbreuk maken op de persoonlijke levenssfeer van mensen. Het wetboek van Strafvordering biedt dan specifieke (opsporings)bevoegdheden.

Naast opsporing is de politie ook belast met de feitelijke handhaving van de openbare orde. Om daar op effectieve wijze uitvoering aan te kunnen geven en om de burgemeester als bevoegd gezag hierover adequaat te kunnen adviseren maakt de politie gebruik van informatie die vaak alleen online te vinden is. Dat betekent dat de politie onderzoek moet doen in online publiek toegankelijke bronnen. Hierbij is al vrij snel sprake van verwerking van persoonsgegevens. Wanneer persoonsgegevens worden verwerkt in het kader van de politietaak valt de verwerking van deze gegevens onder de Wet politiegegevens. Dat betekent dat het raadplegen van deze bronnen aan grenzen is gebonden. De verwerking van persoonsgegevens vormt namelijk een inbreuk op het recht van eerbiediging van de persoonlijke levenssfeer in de zin van artikel 8 van het EVRM, artikel 17 van het Internationaal verdrag inzake burgerlijke en politieke vrijheden, artikel 7 van het EU-Handvest en artikel 10 van de Grondwet. Gelet op de jurisprudentie van het EHRM biedt artikel 3 Politiewet een beperkte juridische grondslag om politiegegevens te kunnen verwerken.

Dit betekent dat bij de toepassing van (politie)bevoegdheden waarmee een min of meer volledig beeld van de persoonlijke levenssfeer wordt verkregen (en dat is in de online-wereld het geval bij het zoeken in niet voor publiek toegankelijke bronnen), een specifieke grondslag is vereist. Bovengenoemde artikelen stellen strenge eisen die erop neer komen dat intensievere en ingrijpender vormen van gegevensverwerking in een aparte (formele) wet dienen te zijn

geregeld. Dat voor een meer dan geringe inbreuk een concrete(re) wettelijke grondslag vereist is en dat artikel 3 Politiewet dan niet voldoet, staat buiten twijfel. Wil de politie handelen binnen de mogelijkheden van deze bepaling dan stelt dat eisen aan de duur en intensiteit van het verzamelen van de onlinegegevens. Uit praktijkvoorbeelden die zijn opgehaald tijdens oriënterende interviews met de politie werd bevestigd dat de politie in de praktijk vaak worstelt met het spanningsveld tussen enerzijds de bescherming van het recht op de bescherming van persoonsgegevens en anderzijds de grote maatschappelijke verantwoordelijkheid de openbare orde te handhaven. In het gesprek werden treffende voorbeelden genoemd rond de aanpak van hooliganisme bij het voetbal en de bestrijding van dealers van (hard)drugs, waarbij gebruik wordt gemaakt van online onderzoek, maar waarbij de (juridische) grenzen van wat wel en niet is toegestaan, niet altijd duidelijk zijn.

Online gegevens verzamelen is een belangrijk onderdeel van de politietaak en dat zal alleen nog maar toenemen. Er wordt veel van de politie gevraagd en daarbij is een helder en bruikbaar juridisch kader nodig. Omdat de politie in dit verband werkt op basis van het algemene artikel 3 van de Politiewet, dat niet gericht is op online informatievergaring, heeft dit tot gevolg dat de politie in elke situatie steeds opnieuw moet afwegen of iets wel of niet proportioneel is en past binnen de beperkte ruimte die dit artikel biedt. Daardoor is de wens ontstaan om de online bevoegdheden van de politie uit te breiden en om aan onduidelijkheden een eind te maken.

1.2 Pleidooien voor verduidelijking en verruiming van online politiebevoegdheden

Uit verschillende onderzoeken blijkt dat de huidige wetgeving op het gebied van gegevensverzameling niet meer voldoet aan de eisen die tegenwoordig worden gesteld aan het politiewerk. Zo blijkt uit onderzoek van Twynstra en Gudde dat door de politie in het kader van de intelligence zowel handmatig als met specifieke software informatie wordt verzameld, maar dat het juridisch kader daarvoor gebaseerd is op politiewerk in de fysieke wereld. De vertaling hiervan naar de online wereld leidt in de praktijk tot veel onduidelijkheden. De onderzoekers van Twynstra bevelen aan tot verduidelijking van de wettelijke kaders te komen.

In een onderzoek naar de avondklokrellen wordt ervoor gepleit dat de politie gebruik moet kunnen maken van online en offline signalen door mee te lezen met wat er op sociale media gebeurt. De onderzoekers doen de aanbeveling dat er een discussie gevoerd moet worden over de vraag of politie en gemeenten meer bevoegdheden moeten krijgen om online in te grijpen bij maatschappelijke onrust of openbare ordeverstoringen.¹

De Commissie-Koops adviseert over de regulering van internetonderzoek door de politie binnen het kader van handhaving van de openbare orde. De commissie adviseert een bredere regeling te treffen die een grondslag biedt voor het verzamelen van persoonsgegevens uit publiek toegankelijke bronnen.²

De minister van Justitie en Veiligheid sluit hierbij aan in haar brief aan de Tweede Kamer wanneer zij stelt dat de politie over voldoende mogelijkheden dient te beschikken om online onderzoek te kunnen doen bij het handhaven van de openbare orde. Wel voegt zij daaraan toe

¹ Een verkennend onderzoek naar online gegevensvergaring door de politie (2022). W. Landman, S. Groothuis Politiewetenschap 126.

² Commissie modernisering opsporingsonderzoek in het digitale tijdperk.

dat mogelijke verruiming van de huidige bevoegdheden dienen te passen binnen de grenzen van legitimiteit, waarborgen en democratische controle. Er dient volgens de minister aldus een zorgvuldige afweging te worden gemaakt tussen de inperking van grondrechten van burgers en de taak die de politie heeft bij de handhaving van de openbare orde.³

1.3 Regelingen in het buitenland

Ter voorbereiding op het concept wetsontwerp dat de politie eigenstandige verdergaande bevoegdheden moet geven bij de inzet van technische hulpmiddelen en bij het doen van online onderzoek in publiek toegankelijke bronnen is het zinvol om te kijken hoe in andere landen het juridisch kader is vormgegeven dat ten grondslag ligt aan de openbare orde taak van de politie en het verzamelen van online informatie. In alle landen van de Europese Unie is de verwerking van persoonsgegevens in het kader van de voorkoming, het onderzoek en de opsporing van strafbare feiten gecodificeerd op basis van EU-richtlijn 2016/680. Tegelijkertijd kennen EU-landen een eigen nationaal wettelijk stelsel van bevoegdheden. Het onderzoek richt zich op de vraag hoe in een aantal EU-landen de betreffende wetten en regels in de praktijk uitpakken en wat daarvan geleerd zou kunnen worden bij het hervormen van het Nederlandse juridische kader omtrent online bevoegdheden van de politie.

1.4 Centrale onderzoeksvragen

Het doel van het onderzoek is het verschaffen van kennis, inzichten en inspiratie uit andere landen ter voorbereiding van een (concept)wetsvoorstel dat de politie eigenstandige bevoegdheden geeft (ook als het gaat om de inzet van technologische hulpmiddelen), werkend binnen een adequaat stelsel van gezag en toezicht. Dit alles ten dienste van het vergaren van (online) gegevens in het kader van de openbare ordetaak, waarbij die vergaring een meer dan geringe inbreuk maakt (dus een grotere inbreuk dan artikel 3 Politiewet toelaat). Het onderzoek dient lessen uit buitenlandse rechtsstelsels respectievelijk casussen te verschaffen.

1. Hoe ziet in een aantal Europese landen het juridisch kader voor het door de politie verzamelen van (online) gegevens ten behoeve van de openbare ordetaak eruit?
2. Wat is bekend over de mate waarin die taakuitvoering zowel effectief als rechtmatig is in deze landen?
3. Welke elementen uit buitenlandse (vigerende of in ontwikkeling zijnde) regelingen worden aanbevolen om in de Nederlandse systematiek toe te passen?

1.5 Opzet van het onderzoek

Het onderzoek is aanvankelijk opgedeeld in drie deelonderzoeken. Deelonderzoek A betreft een overzichtsscan met een globale inventarisatie van regelingen die ten grondslag liggen aan de openbare ordetaak/handhaving van de openbare orde door de politie en de mogelijkheden die deze wettelijke kaders bieden om online informatie te verzamelen. Dit deelonderzoek leidt tot beantwoording van de eerste centrale onderzoeksvraag. Voor deelonderzoek A zijn geselecteerd: Frankrijk, Engeland, Duitsland (deelstaat Hessen), Ierland, Denemarken, Zweden en Spanje.

³ Kamerstukken II 2022-2023, 28 684, nr. 721.

Deelonderzoek B betreft een verdere verdieping van een viertal geselecteerde landen of deelstaten waarbij nader wordt ingegaan op de uitwerking van die wettelijke kaders en de mogelijkheden voor online onderzoek door de politie in de praktijk en de organisatie van het toezicht op de inzet van online politiebevoegdheden. Deelonderzoek B leidt tot beantwoording van de tweede centrale onderzoeksvraag.

Deelonderzoek C gaat in op de vraag welke elementen uit de buitenlandse regelingen geschikt zouden kunnen zijn om ook in Nederland toe te passen, met het oog op de totstandkoming van wetgeving op het terrein van (online) bevoegdheden van de politie. Met deelonderzoek C dient de derde centrale onderzoeksvraag te worden beantwoord.

1.6 Onderzoeksaanpak en -verantwoording

1.6.1 Oriënterende fase

Het onderzoek startte met een viertal oriënterende gesprekken. Deze gesprekken waren bedoeld om beter zicht te krijgen op de Nederlandse situatie en de knelpunten waar wetgevingsjuristen en politie momenteel tegenaan lopen. Daarnaast is in de gesprekken gevraagd naar suggesties voor selectie van casestudylanden. Daartoe is gesproken met een beleidsdossierhouder en wetgevingsjurist van het ministerie van Justitie en Veiligheid. Vervolgens is een groepsgesprek gevoerd met drie adviseurs van de Korpsleiding van de Nationale Politie op het gebied van Intelligence. Tevens is gesproken met een Universitair Hoofddocent digitale veiligheid.

1.6.2 Deelonderzoek A – brede verkenning

Vervolgens is in samenspraak met de begeleidingscommissie een lijst van acht landen opgesteld, te weten: Engeland, België, deelstaat Hessen, Denemarken, Zweden, Ierland en Spanje. Van al deze landen is op basis van deskresearch, open bronnen, wetenschappelijke publicaties en interviews een casestudybeschrijving gemaakt. Onderwerpen die hierbij centraal staan zijn.

- Het doel, de structuur en de reikwijdte van het wettelijk kader van de openbare orde-taak;
- De bevoegdheidsverdeling tussen verschillende partijen/organisaties/instanties;
- De feitelijke handhaving van de openbare orde en de diensten/organisaties die daarbij zijn betrokken;
- Het doel, de structuur en de reikwijdte van het wettelijk kader van het uitoefenen van online politiebevoegdheden;
- De feitelijke uitvoering daarvan en de diensten/organisaties die daarbij betrokken zijn;
- Belangrijke en opvallende inzichten uit de (wetenschappelijke) literatuur.

Hoewel eigenlijk onderdeel van deelonderzoek B, is in aanvulling op bovenstaande onderwerpen voor zover mogelijk ook de inzet van technische hulpmiddelen onderzocht. Bevindingen zijn gebaseerd op openbare bronnen en beschikbare documenten. Voor België geldt dat de bevindingen op dit onderwerp verder zijn uitgediept tijdens gesprekken.

Per land is ernaar gestreefd om ten minste één interview te plannen om de bevindingen op basis van de deskresearch te toetsen en eventueel aan te vullen. Gesproken is veelal met academici die zich bezighouden met openbare orde-vraagstukken in hun land. Alleen voor Zweden is het niet gelukt om in contact te komen met een geschikte gesprekspartner.

Vervolgens is in samenspraak met de begeleidingscommissie een selectie gemaakt voor een verdieping ten aanzien van een drietal landen, te weten: Engeland, België en deelstaat Hessen. In overleg met de begeleidingscommissie is Frankrijk hier later nog aan toegevoegd. In deze landen hebben wij in aanvulling op bovenstaande onderwerpen ook onderzocht op welke wijze het toezicht in deze landen is ingericht. Voor België geldt daarnaast dat er ook uitgebreid gesproken is over de inzet van technische hulpmiddelen.

1.6.3 Deelonderzoek B – verdieping

Het doel van deelonderzoek B is om een verdieping aan te brengen op de hierboven genoemde casestudylanden. Die verdieping zou bereikt moeten worden door interviews met gesprekspartners met de volgende achtergronden:

- Politiemedewerkers met kennis en praktijkervaring op het terrein van openbare ordehandhaving;
- Academics met kennis en expertise op het terrein van openbare ordehandhaving, de inzet van online politiebevoegdheden en technische hulpmiddelen;
- Sleutelinformanten bij een toezichthouder/andere (politie)medewerkers die meer kunnen vertellen over het toezicht op de uitoefening van online politiebevoegdheden; niet-gouvernementele organisaties (NGO's) op het gebied van burgerrechten en privacybescherming;
- Buitenlandse equivalenten van de Autoriteit Persoonsgegevens.

Via gesprekspartners bij de Nationale Politie waarmee contact is geweest in de oriënterende fase is geprobeerd om contact te leggen met de politiediensten in de bovengenoemde landen. Het heeft zowel ons contact bij de politie als de onderzoekers zeer veel inspanningen gekost om met de juiste contactpersonen in de betreffende landen in contact te komen. Hieronder wordt per land kort uiteengezet welke inspanningen zijn geleverd en tot welke contacten en resultaten dit heeft geleid.

Frankrijk

De onderzoekers zijn via een contactpersoon bij het ministerie van Justitie en Veiligheid in contact gebracht met medewerkers van de Nederlandse ambassade in Parijs. Deze medewerkers – met inhoudelijke deskundigheid op het terrein van politiebevoegdheden en intelligence – hebben ons op het goede spoor gezet met het aandragen van relevante openbare Franse bronnen met betrekking tot de inzet van politiebevoegdheden, het toezicht, de governance en het wetgevend kader daaromtrent. Na aanleiding hiervan is de casestudy over Frankrijk opgesteld, waaruit nog een aantal meer operationele vervolgvragen voortvloeide. Onze contactpersonen bij de Nederlandse ambassade in Parijs hebben deze vragen voorgelegd aan de Franse collega's met het verzoek hier schriftelijk, dan wel mondeling een reactie op te geven tijdens een interview. Na meerdere keren rappelleren door onze contactpersoon bij de Franse collega's heeft dit uiteindelijk tot geen reactie geleid en is medewerking uitgebleven. Dat betekent dat een aantal vragen over de meer praktische en operationele aspecten van online informatievergaring door de politie onbeantwoord zijn gebleven.

Daarnaast is een tweetal Franse NGO's benaderd met een verzoek tot medewerking aan een interview. La Quadrature du Net, een van de bekendste Franse digitale rechten- en privacybeschermingsorganisaties en French Data Network (FDN), een non-profit organisatie die zich onder andere bezighoudt met de verdediging van de privacy op het internet en het bevorderen van een open en gedecentraliseerd internet. Beide hebben gereageerd en aangegeven van

wege gebrek aan capaciteit geen medewerking te kunnen verlenen aan het onderzoek. Er is ook contact gezocht met de Franse toezichthouder, de Commission Nationale de l'Informatique et des Libertés. Deze organisatie houdt toezicht op de naleving van de Franse regelgeving op het gebied van gegevensbescherming. De toezichthouder heeft schriftelijk gereageerd op een aantal vragen.

Engeland

Voor de casestudy Engeland hebben we in ruime mate openbare broninformatie kunnen vinden over het Engelse stelsel van openbare ordebevoegdheden, de rol en online bevoegdheden van de politie en het toezicht daarop. Deze informatie diende in het kader van deelonderzoek B verder te worden verrijkt door middel van interviews met gesprekspartners binnen de Engelse toezichthouder op de politie en/of de politie zelf. Hiertoe is via onze contactpersoon binnen de Nederlandse politie die ons ondersteunde bij het leggen van contacten met politieorganisaties in de casestudylanden, contact gezocht met de politie-liaison voor Engeland. Er zijn meerdere pogingen gedaan om ons in contact te brengen met de Engelse toezichthouder (IPCO) op de Engelse autoriteiten (waaronder de politie) met onderzoeksbevoegdheden (investigatory powers). Er is een vertaalde onderzoeksopzet en opdrachtovereenkomst aangeleverd vergezeld van een brief van het WODC om medewerking te verlenen aan het onderzoek. Dit heeft uiteindelijk geen reacties opgeleverd. Tot slot is contact gezocht met een aantal NGO's op gebied van privacy en burgerrechten om ook hun perspectief mee te nemen in het onderzoek. Deze NGO's (Privacy International, Open Rights Group en Big Brother Watch), gaven aan geen tijd/capaciteit te hebben voor medewerking aan het onderzoek.

Duitsland: deelstaten Hessen en Nordrhein-Westfalen

Voor deelstaat Hessen zij we via ons politiecontact in contact gekomen met de de Abteilungsleitung van het Hessisches Landeskriminaliteitsamt. Aanvankelijk werd bereidheid getoond medewerking te verlenen aan het onderzoek. Een Duitstalige notitie is voorgelegd over de bedoeling van het onderzoek, de onderzoeksvragen en het verzoek in contact te komen met een functionaris met praktijkervaring. Na meerdere mailwisselingen is ons verzoek doorgestuurd naar het Hessisches Ministerium van Binnenlandse Zaken met het verzoek iemand voor te dragen die met ons over het onderzoek in gesprek kan. Uiteindelijk hebben we bericht ontvangen dat er niemand is die hierover met ons in gesprek kan, zonder verdere opgaaf van reden.

We hebben vervolgens de focus verlegd naar Nordrhein-Westfalen in de hoop dat we daar wel tot contacten zouden kunnen komen. Dat leek aanvankelijk veelbelovend. Ook hier zijn wederom vertalingen van de onderzoeksopzet, opdrachtovereenkomst en begeleidende brief van het WODC toegezonden om de kans op medewerking te vergroten. Uiteindelijk werd ons gevraagd om onze vragen in het Duits schriftelijk toe te sturen. Dat hebben we gedaan en toegezegd werd dat er een reactie zou komen. Ook hier is, na vele malen rappelleren een reactie uitgebleven.

Er hebben meerdere gesprekken plaatsgevonden met Duitse wetenschappers die zich bezighouden met politiebevoegdheden. De bevindingen van deze gesprekken zijn meegenomen in de casestudy over de deelstaat Hessen. In deze gesprekken ging het vooral over het stelsel en de wetgeving en niet over de feitelijke praktijk. Een van de gesprekspartners, een wetenschapper die zich met dit thema bezighoudt vertelt dat hij wel eens off te record met de politie spreekt over de feitelijke uitvoering, maar dat zijn ervaring is dat de politie zeer terughoudend is met het geven van interviews over operationele praktijken.

Er heeft een gesprek plaatsgevonden met een beleidsmedewerker van de Federal Commissioner for Data Protection and Freedom of Information, de Duitse toezichthouder. Zij zouden ons in contact brengen met de Duitse federale rechedienst (Het Bundeskriminalamt) en de gegevensbeschermingsautoriteiten op Länder niveau. Ondanks inspanningen van deze beleidsmedewerker is dit helaas op niets uitgelopen.

Ook is geprobeerd om contact te leggen met meerdere NGO's met expertise op het terrein van privacy en burgerrechten. Twee van deze organisaties hadden in een vroeg stadium al aangegeven niet te kunnen of willen deelnemen aan het onderzoek. Een andere NGO gaf aan niet mee te willen werken aan ons onderzoek en een andere NGO gaf na meerdere herinneringen aan geen capaciteit te hebben om aan ons onderzoek mee te werken.

België

Voor de casestudy in België hebben we twee gesprekken gevoerd. We hebben met een hoogleraar bestuursrecht aan de Universiteit Gent en een commissaris-onderzoeker bij het Controle-orgaan op de politionele informatie/vrijwillig wetenschappelijk medewerker aan de Vrije Universiteit Brussel gesproken. Vervolgens hebben we geprobeerd om via onze gesprekspartners, mensen die ons doorverwezen, onze eigen contacten en via openbare contactgegevens, in contact te komen met gesprekspartners die zicht hebben op de uitvoeringspraktijk. Met acht personen is geprobeerd om in contact te komen, maar dit heeft – ook na rappelleren – niets opgeleverd. We hebben onder meer contact gezocht met de persoon die verantwoordelijk is voor het departement Intelligence bij de directie operaties bestuurlijke politie van de federale politie. Daarnaast hebben we in het kader van het burgerrechtenperspectief een NGO benaderd, maar ook dat heeft niets opgeleverd. Wel heeft een interview plaatsgevonden met een wetenschapper met expertise op het terrein van de inzet van technische hulpmiddelen bij demonstraties. Deze contactpersoon heeft ons ook op bruikbare literatuur gewezen. We hebben voor de casestudy in België daarnaast veel gebruik kunnen maken van openbare bronnen en literatuur.

1.7 Conclusie dataverzameling

Het is gebleken dat het zeer lastig is om als niet aan de overheid gelieerd onderzoeksbureau medewerking te verkrijgen van overheidsorganisaties in enkele Europese landen. Ondanks de herhaalde verzoeken met uitgebreide toelichting, vertaalde brieven van het WODC waarin het onderzoek is toegelicht en door het WODC is verzocht om medewerking te verlenen aan het onderzoek, heeft dit niet geleid tot de medewerking waarop we hadden gehoopt. Omdat het niet is gelukt om in contact te komen met de politiediensten of andere overheidsorganisaties die op operationeel niveau betrokken zijn bij de uitvoering van online informatievergaring is het niet gelukt om deelonderzoek B uit voeren. Dat heeft ook gevolgen voor het uitvoeren van deelonderzoek C. Daarin diende te worden onderzocht welke elementen uit de stelsels uit de onderzochten landen bruikbaar zou kunnen zijn voor de Nederlandse praktijk.

In de praktijk bleek dat – ondanks beperkingen in de medewerking van buitenlandse (overheids)organisaties – waardevolle aanvullingen mogelijk waren op basis van interviews met academici en andere experts. Deze input is benut om het deskresearch van deelonderzoek A aan te vullen en te verdiepen. In de volgende landen hebben wij gesprekken gevoerd en is de documentstudie aangevuld met informatie uit interviews: Frankrijk, België, Engeland en Duitsland (deelstaat Hessen).

Een verklaring voor het gebrek aan medewerking aan het onderzoek zou mogelijk gelegen kunnen zijn in het feit dat de diensten in de onderzochte landen veelvuldig gebruik maken van online gegevensvergarings bij het handhaven van de openbare orde, maar dat – net zoals in Nederland – er de nodige onduidelijkheid bestaat over de grondslagen voor deze bevoegdheden en over de vraag of deze praktijk in overeenstemming is met het recht in de betreffende landen.

Tot slot merken we op dat de beperkingen in de dataverzameling hebben geleid tot enige mate van onevenwichtigheid in de mate van diepgang van de casestudybeschrijvingen, als gevolg van verschillen in de beschikbaarheid en bruikbaarheid van informatie per land. Dit rapport dient dan ook te worden gelezen als een verkenning en niet als een uitputtende juridische analyse of rechtsvergelijking van de stelsels van openbare ordebevoegdheden en de mogelijkheden daarbinnen voor de politie om online gegevens te vergaren.

1.8 Leeswijzer

In dit rapport worden in de hoofdstukken 2 tot en met 9 beschrijvingen gegeven van de stelsels in Frankrijk, Engeland, Duitsland (Hessen), België, Ierland, Denemarken, Zweden en Spanje. In de beschrijvingen wordt aandacht besteed aan het wettelijk kader voor informatievergaring in het kader van de openbare ordetaak, de actoren die daarbij betrokken zijn, de wijze waarop het toezicht is georganiseerd en de technische hulpmiddelen die hierbij kunnen worden ingezet. In hoofdstuk 10 volgt een korte samenvatting van de bevindingen.

2. Frankrijk

2.1 Organisatie van de openbare ordehandhaving

De Franse politiediensten bestaan uit de Police Nationale (DGPN), de Gendarmerie Nationale (GN) en de Police Municipale (gemeentepolitie). De agenten van de DGPN zijn ambtenaren van de Franse Staat en ressorteren onder het ministerie van Binnenlandse Zaken. De gendarmes (GN) zijn militairen en ressorteren sinds 2009 ook onder het ministerie van Binnenlandse Zaken (daarvoor onder ministerie van Defensie). Zowel de politie als de gendarmerie zijn werkzaam in het hele land en beschikken over dezelfde bevoegdheden. De politie werkt meer in de grote steden en de buitenwijken, terwijl de gendarmerie meer op het platteland te werk gaat. De kleinere steden worden ofwel door de gendarmerie ofwel door de politie bediend.

Parijs (en Marseille) kent ook nog een préfet de police. De préfet de police de Paris (kort préfet de police genoemd) is belast met de veiligheid van personen en goederen op het grondgebied van de agglomeratie Parijs. De préfet de police is belast met voorkomen en bestrijden van criminaliteit en de handhaving van de openbare orde, maar heeft ook taken in verband met het verkeer in en om Parijs en servicegerichte en administratieve taken zoals het afgeven van paspoorten, rijbewijzen en bij de verkrijging van de Franse nationaliteit.

De agenten van de Police municipale zijn lokale ambtenaren in dienst van de burgemeester van de desbetreffende gemeente en spelen een ondergeschikte rol als het gaat om openbare ordehandhaving.

Bij grote en risicovolle gelegenheden waarbij de openbare orde (mogelijk) in het geding is, beschikken de Police Nationale (DGPN), de Gendarmerie en de Préfet de Police elk over een gespecialiseerd korps dat kan worden ingezet bij de handhaving van de openbare orde bij demonstraties, rellen etc., maar ook bij sport- en feestevenementen.⁴ Voor de DGPN is dat de Compagnies Républicaines de Sécurité (CRS).⁵ De CRS maken deel uit van de mobiele veiligheidstroepen, die op het hele nationale grondgebied ingrijpen ter ondersteuning van lokale eenheden, afhankelijk van de behoeften: handhaving en herstel van de orde, bestrijding van

⁴https://www.lemonde.fr/les-decodeurs/article/2019/05/04/crs-gendarmes-mobiles-brav-les-sept-familles-des-forces-de-l-ordre_5458100_4355770.html

⁵ <https://www.police-nationale.interieur.gouv.fr/dossiers/police-nationale-et-autres-forces-de-securite/quelles-sont-differences-entre-police-maitreiosca.fr-POLICE-NATIONALE-MUNICIPALE-ET-GENDARMERIE-QUELS-SONT-LEURS-POUVOIRS>.

criminaliteit, terrorisme of illegale immigratie. Ze kunnen ook plaatsen en mensen beschermen, arresteren of evacueren.

De Gendarmerie beschikt over een vergelijkbare eenheid, Escadron de Gendarmerie Mobile (EGM). De EGM zijn het militaire equivalent van de CRS en zijn verantwoordelijk voor handhaven en herstellen van de openbare orde, ook in risicovolle situaties van stedelijke rellen of gewapende opstanden. Ze treden eveneens op in het buitenland en kunnen worden gemobiliseerd bij buitenlandse operaties.

De Préfet de Police heeft in dergelijke situaties de beschikking over de Compagnie d'Intervention (CI). De eerste Veiligheids- en Interventiecompagnie (CSI) werd in 2003 opgericht door Nicolas Sarkozy om de veiligheid van de wijken van de hoofdstad te waarborgen en om te dienen als versterking tijdens stedelijk geweld. Ook worden ze ingezet voor buurtbeveiliging, evacuaties, huiszoekingen of wegcontroles. Ze zijn mobieler dan de CRS en kunnen arrestaties verrichten.⁶

2.2 Het wettelijk kader voor de uitoefening van de openbare ordetaak

Openbare ordewetgeving

Met de wet *LOI n° 2015-912 relative au renseignement* van 24 juli 2015 is Boek VIII (Livre VIII) van de Code de la sécurité intérieure (CSI) gecreëerd. Boek VIII van de CSI fungeert als de wettelijke basis voor inlichtingenactiviteiten in Frankrijk en is de grondslag voor gegevensvergaring voor alle diensten, dus ook voor de gendarmerie en de Police Nationale wanneer zij de openbare orde handhaven. In boek VIII zijn de doelen van inlichtingen, zoals nationale veiligheid, territoriale integriteit, en de strijd tegen terrorisme neergelegd en worden de technieken die inlichtingendiensten mogen gebruiken bij het verzamelen van inlichtingen beschreven. Ook is in dit wetboek vastgelegd op welke wijze controle wordt uitgevoerd op gegevensverzameling door de inlichtingendiensten.

Het wetgevingstraject startte in 2013 naar aanleiding van het evaluatierapport van het wettelijk kader dat van toepassing is op de inlichtingendiensten.⁷ Uit het rapport volgt dat de wetgeving met betrekking tot inlichtingendiensten in Frankrijk fragmentarisch, gedateerd en ontoereikend was om moderne inlichtingenactiviteiten te reguleren. De Franse inlichtingendiensten opereerden als gevolg hiervan in een juridisch grijs gebied; er ontbrak een wettelijk kader dat bevoegdheden duidelijk definieerde, het toezicht op de inlichten reguleerde en de inzet van nieuwe technologieën (die in de praktijk al wel werden ingezet) legitimeerde.⁸ Het rapport stelt dat er daarom behoefte bestaat aan één duidelijk juridisch kader voor verschillende inlichtingenactiviteiten.

Hoewel het wetgevingstraject in gang was gezet voor de aanslagen op Charlie Hebdo in januari 2015, kan de wet niet los worden gezien van (de dreiging van) het terrorisme en de zorgen over nationale veiligheid.⁹ Reeds sinds de opkomst van het Jihadisme in Europa en de aanslag

⁶ https://www.lemonde.fr/les-decodeurs/article/2019/05/04/crs-gendarmes-mobiles-brav-les-sept-familles-des-forces-de-l-ordre_5458100_4355770.html

⁷ <https://www.assemblee-nationale.fr/14/pdf/rap-info/i1022.pdf>

⁸ Jade Mailliet-Contoz, *Terrorism and Counterterrorism: French Policy after the 2015 Attacks*, 7 december 2018 en Exposé de motifs (memorie van toelichting) code de la sécurité 2015 p.2.

⁹ Zie ook de Exposé de motifs (memorie van toelichting) code de la sécurité 2015. Hier wordt bijvoorbeeld het volgende gesteld: de strijd tegen het terrorisme illustreert de tekortkomingen van het nationale rechtskader.

van 2012¹⁰ is Frankrijk haar veiligheid- en terrorismewetgeving aan het herzien.¹¹ Het wetgevingsproces kwam vervolgens in een stroomversnelling door de aanslagen in Parijs van januari 2015.¹² Door de snelheid van het wetgevingsproces was er minder tijd voor het parlementair debat en juridische analyses, wat leidde tot kritiek van sommige burgerrechtenorganisaties en journalistenverenigingen.¹³

Om tegemoet te komen aan zorgen over grondrechten en privacy, is besloten om de wet aan de Conseil Constitutionnel voor te leggen.¹⁴ Hoewel de meeste bepalingen werden goedgekeurd, werden twee specifieke onderdelen ongrondwettelijk verklaard.¹⁵ Het betrof artikel L. 853-3 (het gebruik van algoritmen door telecommunicatieproviders om verdacht gedrag op netwerken te detecteren) en artikel L. 851-3 (real time toegang tot metadata). Aan deze technieken zijn vervolgens strengere voorwaarden gesteld, waarbij de nadruk werd gelegd op proportionaliteit. Op 24 juni 2015 werd *LOI n° 2015-912 relative au renseignement* aangenomen, waarmee Boek VIII van de CSI is ingevoerd.

Bevoegdheden om online informatie te vergaren met het oog op openbare ordehandhaving

Het vergaren van gegevens door de verschillende inlichtingendiensten is alleen mogelijk als dit de limitatief beschreven doelen dient van artikel L811-3 van de Code de la sécurité intérieur en die worden aangeduid als de 'fundamentele belangen van de natie'.

Deze doelen luiden als volgt.

1. De Nationale onafhankelijkheid, territoriale integriteit en nationale defensie;
2. De grote belangen van het buitenlands beleid, de nakoming van de Europese en internationale verplichtingen van Frankrijk en het voorkomen van elke vorm van buitenlandse inmenging;
3. De grote economische, industriële en wetenschappelijke belangen van Frankrijk;
4. De preventie van terrorisme;
5. Preventie:
 - a) Aanvallen op de republikeinse vorm van instellingen;
 - b) Acties die gericht zijn op het behoud of de heroprichting van groepen die zijn ontbonden op grond van artikel L. 212-1 ;
 - c) collectief geweld dat de openbare vrede ernstig kan ondermijnen;
6. De preventie van georganiseerde criminaliteit en delinquentie;
7. Het voorkomen van de verspreiding van massavernietigingswapens.

De Code de la Sécurité definieert een gelimiteerd aantal inlichtingentechnieken die de daartoe bevoegde instanties kunnen inzetten. Deze technieken worden beschreven in de artikelen L851-1 tot en met L855-1C van titel V, boek VIII van de Code de la sécurité. De inlichtingentechnieken staan hieronder verkort weergegeven. In de wetsartikelen zelf staan de inlichtingentechnieken uitgebreider beschreven.

¹⁰ In 2012 worden bij een terroristische aanslag in Toulouse zeven personen gedood.

¹¹ M. Noordegraaf e.a., terroristische dreiging, noodtoestand en maatschappelijke effecten, WODC, p.41

¹² Jade Maillat-Contoz, Terrorism and Counterterrorism: French Policy after the 2015 Attacks, 7 december 2018, p.3.

¹³ Zie bijvoorbeeld: https://www.amnesty.org/en/latest/news/2015/03/france-new-intelligence-bill-would-pave-the-way-for-extremely-intrusive-surveillance/?utm_source=chatgpt.com.

¹⁴ De Conseil constitutionnel is in Frankrijk een rechterlijke instelling die controleert dat verkiezingen en referenda correct verlopen en dat wetten waarover al is gestemd, in overeenstemming zijn met de grondwet.

¹⁵ Zie Decision no. 2015-713 DC of 23 July 2015, te raadplegen via: https://www.conseil-constitutionnel.fr/en/decision/2015/2015713DC.htm?utm_source=chatgpt.com.

Techniek	Artikel CSI
Toegang achteraf tot verbindingsgegevens. Identificatie van abonnees of inventarisatie van abonnementsnummers of gedetailleerde facturen.	L.851-1
Toegang tot verbindingsgegevens in real-time	L.851-2
Verzamelen van real-time Geo-locaties	L854-4
Onderscheppen van langs elektronische weg verzonden correspondentie	L.852-1
Onderscheppingen via GIC (telefoontap)	L852-1
Onderscheppingen van communicatie door een ISMI-catcher	L. 852-1
Onderschepping van correspondentie verzonden of ontvangen via satelliet	L.852-3
Markering van de locatie van mensen of voorwerpen	L851-5
Verzamelen van verbindingsgegevens door ISMI-catcher	L.851-6
Opnemen van privé gesproken woorden	L853-1
Opnames van beelden op een privélocatie	L853-1
Verzamelen en vastleggen van computergegevens	L853-2
Toegang tot privéplaatsen	L853-3

Deze technieken mogen enkel worden toegepast door *individueel* aangewezen en gemachtigde agenten en worden uitgevoerd onder toezicht van de Nationale Commissie voor de Controle van de Inlichtingentechnieken en, in voorkomend geval, de Raad van State.¹⁶

Artikel L801-1 vormt het basisartikel voor de toepassing van bovengenoemde intelligence-technieken. Het artikel geeft de randvoorwaarden waaraan moet worden voldaan om gegevens te verzamelen. Het artikel, in het Nederlands vertaald, staat hieronder weergegeven.

Artikel L801-1 van boek VIII: 'Inlichtingen'

Respect voor het privéleven, in al zijn componenten, in het bijzonder het briefgeheim, de bescherming van persoonsgegevens en de onschendbaarheid van de woning, wordt door de wet gegarandeerd. De overheid kan er alleen inbreuk op maken in gevallen van noodzaak in het algemeen belang waarin de wet voorziet, binnen de grenzen van de wet en met inachtneming van het evenredigheidsbeginsel.

Tot het verlenen en toepassen op het nationale grondgebied van de in titel V, hoofdstukken I tot en met III van dit boek genoemde technieken voor het vergaren van inlichtingen kan alleen worden besloten indien:

1. Ze worden uitgevaardigd door een daartoe wettelijk bevoegde autoriteit;
2. Ze het resultaat zijn van een procedure in overeenstemming met Titel II van hetzelfde boek;

¹⁶ L.8211 Code de la Sécurité Intérieure.

3. Zij de opdrachten vervullen die zijn toevertrouwd aan de diensten vermeld in artikel L. 811-2 of aan de diensten aangewezen door het decreet van de Raad van State bedoeld in artikel L. 811-4;
4. Ze worden gerechtvaardigd door de bedreigingen, risico's en kwesties die verband houden met de fundamentele belangen van de Natie vermeld in artikel L. 811-3;
5. De inbreuken die zij plegen op de eerbiediging van het privéleven in verhouding staan tot de aangevoerde redenen.

De Nationale Commissie voor de Controle op de Inlichtingentechnieken ziet erop toe, onder de in dit boek vastgelegde voorwaarden, dat deze beginselen worden nageleefd. De Raad van State doet uitspraak over beroepen tegen beslissingen met betrekking tot de toelating en toepassing van deze technieken en over de bewaring van de verzamelde informatie.

Lid 1. Uitvaardiging door een daartoe wettelijk bevoegde autoriteit

Dit artikel houdt in dat alleen daartoe bevoegde autoriteiten een verzoek om inlichtingen en informatie kunnen neerleggen bij een van de inlichtingendiensten (zie paragraaf 1.3)

Lid 2. De procedure

In titel 2 van Boek VIII van de Code de la Sécurité intérieure staat de procedure van toestemming beschreven voor het vergaren van inlichtingen (zie paragraaf 1.4)

Lid 3. De aangewezen diensten

Dit zijn de diensten die op grond van de wet bevoegd zijn om inlichtingen te vergaren.

Lid 4 Doeleinden voor het verzamelen van inlichtingen

De wet formuleert zeven limitatieve doelen waarvoor inlichtingen mogen worden verzameld.

Lid 5 proportionaliteit

De inbreuk op het privéleven staat in verhouding tot het doel waarvoor de inlichtingen worden verzameld.

2.3 De uitvoering van online informatievergaring

Diensten die wettelijk bevoegd zijn op het gebied van het vergaren van inlichtingen kunnen gebruik maken van inlichtingentechnieken. Het inlichtingenwerk is in Frankrijk bij verschillende organisaties neergelegd en verdeeld in een 'eerste cirkel' en een 'tweede cirkel'. Inlichtingendiensten in de eerste cirkel hebben de meeste bevoegdheden als het gaat om het gebruik van inlichtingendiensten. Voor de diensten in de tweede cirkel geldt dat het vergaren van inlichtingen slechts een deel van het werk uitmaken en de opdracht van deze dienst verder strekt dan het vergaren van inlichtingen alleen.

Gespecialiseerde inlichtingendiensten in de eerste cirkel

De eerste cirkel bestaat uit zes autonome gespecialiseerde inlichtingendiensten die van de wetgever de opdracht hebben gekregen om "*informatie met betrekking tot geopolitieke en strategische kwesties, evenals bedreigingen en risico's die het voortbestaan van de natie kunnen beïnvloeden*", te onderzoeken, te verzamelen, te exploiteren en ter beschikking te stellen van de regering. De gespecialiseerde inlichtingendiensten zijn:

- Het directoraat-generaal Externe Veiligheid (DGSE)¹⁷
- De Algemene Directie Binnenlandse Veiligheid (DGSi)¹⁸
- Het Nationaal Directoraat voor inlichtingen en douaneonderzoeken (DNRED)¹⁹
- Het Directoraat van de Militaire Inlichtingendienst (DRM)²⁰
- De Directie Inlichtingen en Defensie Veiligheid (DRSD)²¹
- De dienst voor de verwerking van inlichtingen en actie tegen clandestiene financiële circuits (TRACFIN)²²

Diensten in de tweede cirkel

De twintig diensten in de tweede cirkel kunnen ook inlichtingen verzamelen, maar zijn daar niet primair mee belast en voeren dus ook andere (politie)taken uit. Zij mogen slechts gebruik maken van enkele van de (doorgaans minder ingrijpende) inlichtingentechnieken waarin de wet voorziet en slechts voor een beperkt aantal doeleinden. Het verschilt per dienst van welke technieken gebruik mag worden gemaakt. Deze diensten zijn onderdeel van de:

- Algemene Directie van de Nationale Politie (DGPN)²³
- Algemene Directie van de Nationale Gendarmerie
- Prefectuur van Politie (Préfet de Police)
- Gevangenisadministratie

In de tweede cirkel zitten twintig diensten. Vier van deze diensten die een exclusieve inlichtingenuitvoering hebben en onder een van vier bovengenoemde diensten vallen zijn de:²⁴

- Nationale Directie van de Territoriale Inlichtingendienst binnen de Algemene Directie van de Nationale Politie (DNRT)²⁵
- Inlichtingendirectie van de Prefectuur van Politie (DRPP)²⁶
- Onderdirectie Operationele Anticipatie binnen de Algemene Directie van de Nationale Gendarmerie (SDAO)²⁷
- Nationale Inlichtingendienst van het Penitentiaire Wezen binnen de directie van de gevangenisadministratie (SNRP)²⁸

DNRT

De DNRT is een onderdeel van de DGPN waarin de police nationale en gendarmerie samenwerken op het gebied van gegevensvergaring. DNRT draagt bij aan het voorkomen van gewelddadig extremisme. Het centraliseert en analyseert informatie op institutioneel, economisch en sociaal gebied, en op alle gebieden die van belang kunnen zijn voor de openbare orde, met inbegrip van geweld.²⁹ DNRT verzamelt gegevens over mogelijke verstoringen van de openbare orde op het gehele grondgebied van Frankrijk, inclusief overzeese gebiedsdelen, exclusief de regio (prefecture en aangrenzende gebieden van) Parijs.³⁰

¹⁷ La Direction générale de la sécurité extérieure.

¹⁸ La Direction générale de la sécurité intérieure.

¹⁹ La Direction nationale du renseignement et des enquêtes douanières.

²⁰ La Direction du renseignement militaire.

²¹ La direction du renseignement et de la sécurité de la défense.

²² Le service à compétence nationale dénommé « traitement du renseignement et de l'action contre les circuits financiers clandestins ».

²³ La Direction générale de la police nationale.

²⁴ <https://www.cnctr.fr/services-de-renseignement>.

²⁵ La direction nationale du renseignement territorial.

²⁶ La direction du renseignement de la préfecture de police.

²⁷ La sous-direction de l'anticipation opérationnelle.

²⁸ Le service national du renseignement pénitentiaire.

²⁹ <https://www.cnctr.fr/services-de-renseignement>

³⁰ <https://www.police-nationale.interieur.gouv.fr/nous-decouvrir/notre-organisation/organisation/direction-nationale-du-renseignement-territorial-dnrt>

DRPP

De DRPP, een dienst die onder het gezag van de prefect van politie staat, is belast met het onderzoeken en analyseren van informatie die bedoeld is om de prefect te informeren op institutioneel, economisch en sociaal gebied en op alle gebieden die van belang kunnen zijn voor de openbare orde en de werking van de instellingen in de hoofdstad Parijs en de omliggende departementen van Hauts-de-Seine, Seine-Saint-Denis en Val-de-Marne.³¹

SDAO

De SDAO, die onder het gezag van de directeur-generaal van de nationale gendarmerie staat, draagt bij aan de inlichtingenopdracht van de gendarmerie op het gebied van defensie, nationale veiligheid en in het bijzonder de openbare orde.³² SDAO is een dienst die 24/7 actief en in real-time informatie analyseert en daarmee de operatie bedient. Elk thema dat gevolgen of impact kan hebben op de openbare orde de algemene veiligheid kan worden onderzocht.³³

SNRP

De missie van de SNRP is het onderzoeken, verzamelen, exploiteren, analyseren en verspreiden van informatie en inlichtingen die risico's kunnen opleveren voor schade aan de fundamentele belangen van de natie, de veiligheid van gevangenen, gezondheidsinstellingen die bedoeld zijn om gedetineerden op te vangen en gevangendienst. De SNRP rapporteert aan het ministerie van Justitie.³⁴

2.4 Toestemming voor en controle op informatievergaring

La Commission Nationale de Contrôle des Techniques de Renseignement

La Commission Nationale de Contrôle des Techniques de Renseignement (hierna: de CNCTR) is een bestuurlijke toezichhoudende autoriteit. Deze autoriteit ziet erop toe dat de technieken voor het verzamelen van inlichtingen door de verschillende inlichtingendiensten op het nationale grondgebied worden toegepast in overeenstemming met de wet.³⁵

De CNCTR is opgericht op grond van de Code de la Sécurité intérieure. Deze autoriteit bestaat uit negen leden. Vier leden zijn afkomstig uit het parlement: twee afgevaardigden worden aangewezen door de voorzitter van de Nationale Vergadering en twee senatoren worden aangewezen door de voorzitter van de Senaat. Twee leden zijn afkomstig uit de Raad van State en worden aangewezen door diens Vice-President.³⁶ Twee leden van het Hof van Cassatie³⁷ worden aangewezen door de (eerste) voorzitter van het Hof en de Procureur Generaal bij het Hof. Eén lid wordt door de President benoemd.³⁸ Dit lid is expert op het gebied van elektronische communicatie. De voorzitter van de CNCTR wordt door de President bij Decreet benoemd en gekozen uit de leden afkomstig van de Raad van State en het Hof van Cassatie. Voorafgaand aan deze benoeming wordt advies ingewonnen van de Nationale Vergadering en de Senaat. Deze consultatie is openbaar.³⁹

³¹ <https://www.cnctr.fr/services-de-renseignement>.

³² <https://www.cnctr.fr/services-de-renseignement>.

³³ <https://www.gendarmerie.interieur.gouv.fr/gendinfo/dossiers/la-dggn-operationnelle/presentation-de-la-sous-direction-de-l-anticipation-operationnelle?>

³⁴ <https://www.cnctr.fr/services-de-renseignement>.

³⁵ Artikel L. 833-1.

³⁶ De leden hebben minstens het niveau van Staatsraad.

³⁷ Ieder buiten de hiërarchie van het Hof.

³⁸ Op voorstel van de voorzitter van de regelgevende autoriteit voor elektronische communicatie en post.

³⁹ Artikel L. 831-1.

De leden worden benoemd voor een ambtsperiode van zes jaar, behoudens de leden afkomstig uit het parlement. Daarvan loopt de termijn gelijk met de duur van hun mandaat. De helft van de leden van de Raad van State en het Hof van Cassatie worden om de drie jaar vernieuwd. De ambtsperiode van de leden kan in beginsel niet worden verlengd. Er is een gelijke vertegenwoordiging van mannen en vrouwen.⁴⁰

De CNCTR wordt ondersteund door een eigen ambtelijke organisatie onder leiding van een secretaris-generaal. Deze wordt aangesteld door de voorzitter van de CNCTR. De CNCTR beschikt naast personele middelen ook over technische en financiële middelen.⁴¹

Onafhankelijkheid

De CNCTR opereert onafhankelijk van de regering en het parlement. De onafhankelijkheid wordt geborgd in de wijze waarop de negen leden van de autoriteit worden benoemd. Daarnaast wordt de onafhankelijke positie onderstreept doordat de leden geen instructie mogen ontvangen van enig autoriteit.⁴² Ook geldt vanuit die optiek dat de functie van lid onverenigbaar is met enig belang, direct of indirect, in de diensten die gemachtigd zijn om de in de wet opgenomen technieken toe te passen of in de activiteit van een van de personen genoemd in artikel L. 34-1 II van het Wetboek van Posthandel en Elektronische Communicatie, evenals in artikel 6, 1 en 2 van I, van wet nr. 2004-575 van 21 juni 2004 voor het vertrouwen in de digitale economie. De functie van lid is eveneens onverenigbaar met elke voltijdse beroepsactiviteit of andere openbare betrekking en elk verkozen ambt, met uitzondering van de vier leden afkomstig uit het parlement.⁴³ Deze beperking geldt ook voor de voorzitter van de CNCTR.⁴⁴

De CNCTR stelt een Reglement van Orde op⁴⁵, waarin ethische spelregels worden neergelegd. Dit reglement geldt voor de leden en ambtenaren. De ethische spelregels geven invulling aan loyaliteit, vertrouwelijkheid, onpartijdigheid en onafhankelijkheid. Deze spelregels gelden zowel tijdens als ook na afloop van de ambtsperiode of het dienstverband.

Taken

De wet definieert het gebruik van inlichtingentechnieken voor het verzamelen van inlichtingen op het Franse grondgebied en welke inlichtingentechnieken door welke inlichtingendienst mogen worden gebruikt.

Advisering aan de premier

De CNCTR heeft een adviserende taak richting de premier over het gebruik van de in de wet genoemde inlichtingentechnieken. Deze advisering vindt plaats voorafgaand aan de vergunningverlening door de premier (advisering a priori). Daarnaast is de CNCTR ook bevoegd om het gebruik van inlichtingentechnieken achteraf te controleren (controle a posteriori). De CNCTR gaat in het kader van de voorafgaande advisering en de controle achteraf na of:

- de inzet van de inlichtingentechnieken uitsluitend plaatsvindt in het kader van de uitoefening van de taken die aan de inlichtingendiensten zijn toegekend;
- de inzet van inlichtingentechnieken kan worden gerechtvaardigd door de bedreigingen, risico's en kwesties die verband houden met de fundamentele belangen van de Natie, zijnde de nationale onafhankelijkheid, territoriale integriteit en nationale defensie; belangen inzake buitenlands beleid, de nakoming van de Europese en internationale

⁴⁰ Artikel L. 831-1.

⁴¹ Artikel L. 832-4.

⁴² Artikel L. 832-1.

⁴³ Artikel L. 832-2.

⁴⁴ Artikel L. 832-2.

⁴⁵ Artikel L. 832-3.; Délibération, no. 2/2017 du 23 mars 2017, Règlement intérieur.

verplichtingen van Frankrijk en het voorkomen van elke vorm van buitenlandse inmenging; de economische, industriële en wetenschappelijke belangen van Frankrijk; het voorkomen van terrorisme; het voorkomen van aanvallen op de republikeinse vorm van instellingen; het voorkomen van acties die gericht zijn op het in stand houden of opnieuw samenstellen van groepen die zijn ontbonden en het voorkomen van collectief geweld dat de openbare orde en veiligheid ernstig kan ondermijnen; het voorkomen van georganiseerde criminaliteit en het voorkomen van de verspreiding van massavernietigingswapens;⁴⁶

- de inbreuken die door de inzet van inlichtingentechnieken worden gepleegd op de eerbiediging van het privéleven in verhouding staan tot de aangevoerde redenen.⁴⁷

Gevraagd en ongevraagd advies

De CNCTR kan te allen tijde aan de premier opmerkingen richten die zij nuttig acht. Deze opmerkingen worden door de premier medegedeeld aan de Parlementaire delegatie voor Inlichtingen.⁴⁸ Daarnaast beantwoordt de CNCTR adviesverzoeken van de premier, de voorzitter van de Nationale Vergadering, de voorzitter van de Senaat en de parlementaire delegatie voor inlichtingen.⁴⁹

Voorafgaande advisering (advisering a priori)

De inzet van inlichtingentechnieken is onderworpen aan de voorafgaande toestemming van de premier in de vorm van een vergunning, afgegeven na advies van de CNCTR.⁵⁰ Het gebruik van inlichtingentechnieken zonder goedkeuring van de premier is strafbaar.⁵¹ In 2023 werden 94.902 verzoeken om een vergunning ingediend betreffende 24.209 subjecten.

De wet stelt eisen, waaraan het verzoek dient te voldoen. De reden daarvoor is dat de verzoeken zo spoedig mogelijk kunnen worden behandeld en de doeltreffendheid van de advisering kan worden gegarandeerd. In het verzoek worden de toe te passen techniek(en); de dienst waarvoor de technieken worden ingezet; het (de) nagestreefde doel(en) daarvan; de reden(en) voor de maatregelen; de geldigheidsduur van de vergunning en de betrokken perso(n)en(en), plaats(en) of voertuig vermeld. Wanneer de aanvraag strekt tot verlenging van een vergunning, worden de redenen uiteengezet waarom die verlenging gerechtvaardigd is in het licht van het doel of de nagestreefde doeleinden.⁵²

Het verzoek om een dergelijke vergunning dan wel een verzoek tot verlenging van een eerder afgegeven vergunning wordt meegedeeld aan de voorzitter van de CNCTR of, bij afwezigheid van de voorzitter, aan een van de leden afkomstig van de Raad van State of het Hof van Cassatie. Binnen vierentwintig uur wordt een advies uitgebracht en wordt het advies onverwijld medegedeeld aan de premier.⁵³ Dit advies wordt uitgebracht door de voorzitter of door een lid afkomstig van de Raad van State of het Hof van Cassatie. Deze adviezen worden vervolgens ter beschikking gesteld aan alle leden van de CNCTR.⁵⁴

In de praktijk hanteert de CNCTR een zogenoemde prioriteitsprocedure om te kunnen reageren op operationele behoeften die dringende advisering behoeven. Bij de toepassing van deze

⁴⁶ Artikel L. 811-3.

⁴⁷ Artikel L. 801-1.

⁴⁸ Artikel L. 833-10.

⁴⁹ Artikel L. 833-11.

⁵⁰ Artikel L. 821-1 en Artikel 8.21-3.

⁵¹ Artikel L. 811-2.

⁵² Artikel L. 821-2.

⁵³ Artikel L. 821-3.

⁵⁴ Artikel L. 832-3.

procedure kan binnen een tijdsbestek van doorgaans minder dan een uur advies worden uitgebracht. Deze procedure kan ook 's-nachts of in het weekend worden doorlopen en vereist een goede samenwerking tussen de verschillende actoren in het proces, waaronder de premier. Getoetst wordt of elk verzoek voldoet aan de criteria voor interventie, zoals proportionaliteit en urgentie.⁵⁵

Elke nieuwe of ernstige kwestie wordt verwezen naar de plenaire vergadering of de vergadering in beperkte omvang. De plenaire vergadering omvat alle leden. De vergadering in beperkte samenstelling bestaat enkel uit de leden van de Raad van State, het Hof van Cassatie en het expert-lid. Beide gremia worden voorgezeten door de voorzitter.⁵⁶ Deze gremia kunnen ook worden bijeengeroepen wanneer de voorzitter dan wel de hiervoor genoemde leden van oordeel zijn dat de geldigheid van de aanvraag niet zeker is.

Wanneer het verzoek in een van beide vergaderingen wordt behandeld, wordt de premier hiervan onverwijld in kennis gesteld en wordt het advies binnen tweeënzeventig uur uitgebracht. De plenaire vergadering en de vergadering in beperkte omvang kunnen slechts geldig beraadslagen indien er respectievelijk ten minste vier en drie leden aanwezig zijn. De beslissingen worden genomen door een meerderheid van de aanwezige leden. In geval de stemmen staken, is de stem van de voorzitter doorslaggevend. De plenaire vergadering komt ten minste eenmaal per maand bijeen.⁵⁷

Van een ernstige kwestie is in ieder geval sprake wanneer advies wordt gevraagd ten aanzien van een verzoek gericht op een parlements lid, een magistraat, een advocaat of een journalist. Een dergelijk verzoek kan niet worden ingediend, wanneer het verzoek om inzet van inlichtingentechnieken zich richt op de uitoefening van zijn mandaat of zijn beroep. Wanneer een dergelijk verzoek betrekking heeft op een van deze personen of op zijn voertuigen, kantoren of woningen, wordt het advies van de CNCTR in plenaire en voltallige zitting behandeld.⁵⁸

Indien binnen de gestelde termijnen geen advies is toegezonden aan de premier, wordt het advies geacht te zijn uitgebracht.⁵⁹ Dit lijkt te moeten worden geduid als ware het een *Lex silencio positivo*.

Bij de advisering door de CNCTR wordt, nadat de ontvankelijkheid van het verzoek is beoordeeld, getoetst⁶⁰ of:

- het doel van de te verzamelen informatie inderdaad valt onder een van de zeven categorieën van fundamentele belangen van de natie, zoals hiervoor genoemd, om het gebruik van inlichtingentechnieken te rechtvaardigen;
- het aannemelijk is dat de betrokkene persoonlijk betrokken is bij activiteiten die de fundamentele belangen van de Natie bedreigen of, indien de specifieke materiewetgeving daarin voorziet, dat mensen in de omgeving van een persoon op geloofwaardige wijze relevante informatie kan verstrekken met betrekking tot deze belangen. De motivering van het verzoek moet voldoende onderbouwd en gedetailleerd zijn;
- het gebruik van de gevraagde inlichtingentechniek in verhouding staat tot het concrete geval: bij elk verzoek weegt de CNCTR enerzijds de ernst van de inbreuk op de

⁵⁵ Zie 7e Rapport d'activité 2022, p. 16-17.

⁵⁶ Artikel L. 831-2.

⁵⁷ Artikel L. 832-3.

⁵⁸ Artikel L. 821-7.

⁵⁹ Artikel L. 821-3.

⁶⁰ <https://www.cnctr.fr/contrôle-prealable>

- persoonlijke levenssfeer als gevolg van de toepassing van de betrokken techniek af en anderzijds de door de auteur aangevoerde redenen en de door hem nagestreefde doeleinden;
- bij het gebruik van de meest ingrijpende technieken de inzet daarvan de enige manier is om de gevraagde informatie te verzamelen: de CNCTR toetst daarbij aan het subsidiariteitsbeginsel.

Wanneer de premier na advisering door de CNCTR een vergunning verleent is dat voor een termijn van maximaal vier maanden. Naast het verzoek wordt ook de vergunning geregistreerd door het kabinet van de premier. Het register wordt beschikbaar gesteld aan de CNCTR. De premier kan ook na een negatief advies van de CNCTR een vergunning verlenen. De premier vermeldt de redenen waarom het advies niet is opgevolgd. De premier stelt de vergunning onverwijld ter beschikking aan onder meer de CNCTR.⁶¹ De CNCTR kan in dat geval bij de Raad van State beroep in stellen tegen de verleende vergunning.⁶²

In het geval de vergunning ziet op de inzet van inlichtingentechnieken ten aanzien van een parlementslid, een magistraat, een advocaat of een journalist ontvangt de CNCTR automatisch de transcriptie van ingezette technieken, zodat kan worden gecontroleerd of de inzet niet ziet op de toepassing van het gegeven mandaat of de uitoefening van diens beroep.⁶³

In het geval van absolute spoedeisendheid kan de premier onder voorwaarden een vergunning verlenen zonder voorafgaand advies van de CNCTR. In dat geval zendt de premier de CNCTR binnen een termijn van maximaal vierentwintig uur na het verlenen van de vergunning de benodigde informatie, waaronder de aard van de absolute spoedeisendheid die de verlening van de vergunning rechtvaardigt.⁶⁴

Wanneer zich een noodsituatie voordoet die ziet op een onmiddellijke dreiging of zich een zeer hoog risico voordoet wat maakt dat de operatie niet op een later tijdstip kan worden uitgevoerd, mogen bepaalde inlichtingentechnieken bij wijze van uitzondering zonder vergunning van de premier worden gebruikt. De premier en onder meer de CNCTR kunnen te allen tijde bevelen dat de toepassing van de betrokken technologie wordt onderbroken en dat de verzamelde informatie onverwijld wordt vernietigd. Binnen achtenveertig uur wordt vergunning verleend, nadat de CNCTR advies heeft uitgebracht in het licht van de beschikbaar gestelde informatie, waaronder de rechtvaardiging van het gebruik van de noodprocedure.⁶⁵

De procedure voor een situatie die vraagt om absolute spoedeisendheid is niet van toepassing wanneer een verzoek ziet op een parlementslid, een magistraat, een advocaat of een journalist. De noodsituatie is in dat geval slechts van toepassing in het geval er ernstige redenen zijn om aan te nemen dat de betrokkene handelt in opdracht van een buitenlandse mogendheid of in het kader van een terroristische groepering of een criminele organisatie.⁶⁶

Controle achteraf (controle a posteriori)

De CNCTR kan te allen tijde de premier aanbevelingen doen om de toepassing van een inlichtingentechniek te onderbreken en de verkregen data te vernietigen. Tot een dergelijke

⁶¹ Artikel L. 821-4.

⁶² Artikel L. 833-8 in samenhang gezien met artikel 841-1, onderdeel 2.

⁶³ Artikel L. 821-7.

⁶⁴ Artikel L. 821-5.

⁶⁵ Artikel L. 821-6.

⁶⁶ Artikel L. 821-7.

aanbeveling wordt gekomen, indien de vergunning of de toegepaste inlichtingentechniek in strijd is met de wet. Het kan daarbij ook gaan om de verdere verwerking van de verkregen gegevens.⁶⁷

De CNCTR voert ambtshalve of wanneer zij een klacht ontvangt van een persoon die wenst na te gaan of een inlichtingentechniek onrechtmatig op hem wordt toegepast, een controle uit op de inzet van de inlichtingentechniek(en) om na te gaan of deze in overeenstemming met de wet is of wordt toegepast. Zij deelt de persoon mee dat de nodige controles zijn uitgevoerd zonder de uitvoering ervan te bevestigen of te ontkennen.⁶⁸

De controle achteraf is volgens de CNCTR van cruciaal belang, gezien de zorg die er bij de CNCTR is voor een groeiende kloof tussen de beperkte middelen van de CNCTR en het gebruik van steeds verdergaande en invasieve methoden die het mogelijk maken een grote hoeveelheid gegevens te verzamelen.⁶⁹

De CNCTR onderscheidt ten aanzien van de controle achteraf drie dimensies, namelijk i) inzicht in de gegevens die verzameld zijn door middel van inlichtingentechnieken, ii) de regelmatige controle van de inzet van deze technieken waar het gaat om een parlementslid, een magistraat, een advocaat of een journalist en iii) een meer educatieve en relationele dimensie, waardoor beter zicht wordt gekregen in de praktijk en de context waarin door de diensten gewerkt wordt en het contact met de operationele medewerkers te onderhouden en daarmee mogelijke misverstanden weg te nemen of te voorkomen.⁷⁰

Bevoegdheden

Ten behoeve van de uitvoering van de advies- en controletaak is de CNCTR bevoegd om:

- mededeling te ontvangen van alle verzoeken;
- permanente, volledige en rechtstreekse toegang te hebben tot onder meer de verklaringen, registers, verzamelde informatie en transcripties als bedoeld in de wet, tot de ingezette systemen voor de traceerbaarheid van de verzamelde informatie en tot de lokalen waar deze informatie aanwezig is;
- te allen tijde, op haar verzoek, op de hoogte te worden gebracht van de uitvoering van lopende vergunningen;
- de premier te verzoeken om, behoudens uitzonderingen, alle informatie die nodig is voor de uitvoering van de taken van de CNCTR, ook wanneer de toegepaste techniek voor het verzamelen van inlichtingen niet het voorwerp is geweest van een verzoek;
- bij de premier alle of een deel van de verslagen van de Inspectie van de Inlichtingendiensten op te vragen, alsook de verslagen van de Algemene Inspectie van de Ministeries met betrekking tot de diensten die onder hun bevoegdheid vallen, in het kader van haar taakuitoefening.

Ministers, overheidsinstanties en ambtenaren nemen alle nodige maatregelen om de werkzaamheden van de CNCTR te vergemakkelijken. Het belemmeren van de actie van de CNCTR wordt bestraft met een jaar gevangenisstraf en een boete van € 15.000.⁷¹

⁶⁷ Artikel L. 833-6.

⁶⁸ Artikel L. 833-4.

⁶⁹ Zie 8e Rapport d'activité 2023, p. 48.

⁷⁰ Zie 8e Rapport d'activité 2023, p. 48.

⁷¹ Artikel L. 833-2.

Geheimhouding

De advies- en controletaak ziet op werkzaamheden van inlichtingendiensten die vallen onder de geheimhoudingsverplichting zijnde *le secret de la défense nationale*. De leden en medewerkers van de commissie nemen deze geheimhouding in acht en zijn daartoe ook wettelijk verplicht. Deze verplichtingen blijven van kracht na het einde van het mandaat of dienstverband. Zaken die onder de geheimhoudingsverplichting vallen, mogen niet worden besproken met een dienst of een medewerker die er geen kennis van hoeft te hebben en er niet voor gemachtigd is.⁷²

Verantwoording

De CNCTR wordt gezien als een *Trusted Third Party* voor de beide kamers van het parlement aan wie de CNCTR verantwoording aflegt. De noodzaak van een *Trusted Third Party* wordt toegeschreven aan de scheiding der machten – het toezicht op de inlichtingendiensten kan alleen worden uitgevoerd door een orgaan dat losstaat van het parlement – en de eerbieding van *le secret de la défense nationale*. De CNCTR brengt jaarlijks verslag uit aan het parlement over haar werkzaamheden en haar bevindingen over het gebruik door inlichtingendiensten van inlichtingentechnieken zonder informatie uit de operatie te onthullen. In het jaarverslag wordt ook melding gemaakt van het aantal bij haar ingediende aanvragen en uitgebrachte adviezen, de bij haar ingediende klachten, de aanbevelingen die zij de premier heeft gedaan en de mate waarin deze zijn opgevolgd, de opmerkingen die zij aan de premier heeft gericht en de adviezen die zij op verzoek heeft uitgebracht, het aantal maal dat de spoed- en noodprocedure is gebruikt en het aantal beroepen dat bij de Raad van State is ingediend.⁷³

Verhouding CNCTR en CNIL

De CNIL (Commission Nationale de l'Informatique et des Libertés) houdt toezicht op de bescherming van persoonsgegevens ter uitvoering van de Algemene verordening gegevensbescherming (EU-verordening 2016/679) en de Franse uitvoeringswet van deze Europese verordening. In deze uitvoeringswet is ook de EU-richtlijn 2016/680 is geïmplementeerd.⁷⁴

Bij de totstandkoming van de onderhavige wet heeft de CNIL als wetgevingsadviseur een advies uitgebracht.⁷⁵ Gelet op de aard en complexiteit van de door de inlichtingendiensten verwerkte persoonsgegevens is volgens de CNIL een strengere controle noodzakelijk dan thans door de premier en de CNCTR wordt uitgevoerd. Deze controle dient te zien op de voorwaarden voor de verwerking van de verzamelde persoonsgegevens en of dit in overeenstemming is met het gegevensbeschermingsrecht. De CNIL hield ten tijde van de inwerkingtreding van de wet geen toezicht op deze verwerking. De CNIL stelt voor om dit toezicht op deze verwerkingen mogelijk te maken en daarbij de CNCTR te betrekken om de vertrouwelijkheid van de data te borgen, omdat dergelijke controlebevoegdheden een essentiële aanvullende garantie vormen in overeenstemming met de doelstellingen van de wet.

Uit de parlementaire behandeling volgt dat dit aspect van het advies van de CNIL onderwerp is geweest van de beraadslagingen in de Nationale Vergadering, maar uiteindelijk niet heeft geleid tot een wijziging van het wetsvoorstel.

⁷² Artikel 3 van het Reglement van Orde.

⁷³ Artikel L. 833-9.

⁷⁴ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

⁷⁵ Zie het advies van de CNIL van 5 maart 2015 over het wetsvoorstel inzake inlichtingen, p. 9-11 (<https://www.cnil.fr/sites/cnil/files/typo/document/D2015-078-PJLRenseignement.pdf>)

3. Engeland

3.1 Organisatie van de openbare ordehandhaving

In het Verenigd Koninkrijk is de verantwoordelijkheid voor de handhaving van de openbare orde verdeeld over verschillende instanties op verschillende niveaus, waaronder lokale, regionale en nationale autoriteiten. Engeland heeft op basis van *The Police Act 1996* een centraal politiebestedel met aan het hoofd *The National Crime Agency* en daaronder lokale politiekorpsen.⁷⁶ Lokale politiekorpsen, onder leiding van een *Chief Constable*, zijn belast met het waarborgen van de openbare veiligheid op lokaal niveau. Zij treden op bij demonstraties, evenementen, rellen en andere situaties waarbij de openbare orde in het geding is. Deze politiediensten, zoals de *Greater Manchester Police*, *West Midlands Police*, of *Thames Valley Police*, hebben als taak de openbare orde te handhaven binnen hun geografische grenzen. Over het algemeen vereist de handhaving van de openbare orde een nauwe samenwerking tussen deze instanties, met de lokale politie als sleutelfiguur op het gebied van dagelijkse operaties.

In Engeland staat de lokale politie onder het gezag van de Chief Constable (hoofdcommissaris) van het betreffende politiekorps. De Chief Constable is het hoogste bevelhebber van het politiekorps en heeft de verantwoordelijkheid voor de algemene en dagelijkse leiding van het politiekorps en de uitvoering van de politieactiviteiten binnen hun jurisdictie, waaronder het handhaven van de openbare orde, het voorkomen en opsporen van misdrijven en het waarborgen van de veiligheid binnen de toegewezen regio.

Naast de Chief Constable die verantwoordelijk is voor operationele aangelegenheden, houdt de *Police and Crime Commissioner (PCC)* namens de samenleving toezicht op het politiekorps. De PCC is een gekozen functionaris en heeft als doel de belangen van de gemeenschap te vertegenwoordigen en het politiebeleid te beïnvloeden. De relatie tussen de Chief Constable en de PCC vormt een belangrijk aspect van het Engelse politiebestedel. De burgemeester heeft in het Engelse bestel geen direct gezag over de operationele beslissingen van de politie.

⁷⁶ WRR, *Politiefunctie in een veranderende omgeving – Appendix B, Engeland en Wales*. 2021.

3.2 Het wettelijk kader voor de uitoefening van de openbare ordetaak

Openbare ordewetgeving

In het Verenigd Koninkrijk vindt de openbare ordehandhaving plaats binnen het kader van verschillende wetten en regelgeving. Een aantal wetten is hierbij met name van belang. De *Public Order Act 1986* voorziet in bepalingen met betrekking tot openbare orde met inbegrip van het reguleren van demonstraties en het voorkomen van wanordelijk gedrag. De wet stelt bevoegdheden vast voor de politie en autoriteiten om de openbare orde te handhaven.

De *Police and Criminal Evidence Act 1984* regelt basisrechten en politietaken. De wet reguleert bijvoorbeeld de aanhouding van verdachten en het gebruik van dwang. De *Criminal Justice and Public Order Act van 1994* breidde de bevoegdheden van de politie uit om op te kunnen treden tegen krakers en verstoringen van de openbare orde, evenals het reguleren van muziekfestivals en grote bijeenkomsten. De *Football Spectators Act 1989* richt zich specifiek op voetbalrellen en stelt bepalingen vast om de veiligheid bij voetbalevenementen te waarborgen.

De *Human Rights Act 1998* is geen specifieke wet is voor openbare orde, maar regelt de waarborgen van de rechten en vrijheden van individuen.

Bevoegdheden om online informatie te vergaren met het oog op openbare ordehandhaving

De bevoegdheid voor overheidsinstanties, waaronder de politie, om (online) informatie te vergaren is geregeld in de *Investigatory Powers Act 2016*⁷⁷ (IPA). Deze wet heeft tot doel een uitgebreid wettelijk kader te bieden voor het reguleren van de bevoegdheden van de overheid met betrekking tot surveillance, onderschepping van communicatie en het verzamelen van informatie. De doeleinden waarvoor op basis van deze wet informatie kan worden vergaard zien zowel op de bestrijding van ernstige criminaliteit en terrorisme, als op openbare ordehandhaving. De IPA is een complexe wet en het gebruik van bevoegdheden is onderhevig aan strikte wettelijke en procedurele vereisten. Bepalingen uit deze wet kunnen relevant zijn voor specifieke situaties, afhankelijk van het type bevoegdheid dat wordt toegepast.

Verder is relevant de *Regulation of Investigatory Powers Act 2000* (RIPA), die onder meer de toestemming/autorisatie regelt voor het uitvoeren van surveillancetechnieken (covert surveillance) door overheidsinstanties. De wetgever introduceerde deze wet vanwege de Human Rights Act 1998 die *public authorities* opdraagt te handelen in overeenstemming met het Europees Verdrag voor de Rechten van de Mens (EVRM) en meer in het bijzonder artikel 8, het recht op privéleven.

Hoewel RIPA geen expliciete bepaling kent over online activiteiten regelt de wet dat surveillancetechnieken altijd noodzakelijk, proportioneel en in overeenstemming met de mensenrechten moeten zijn.⁷⁸ In een guideline van de *Lancaster City Council* wordt procedure omtrent toestemming op grond van RIPA als volgt omschreven:

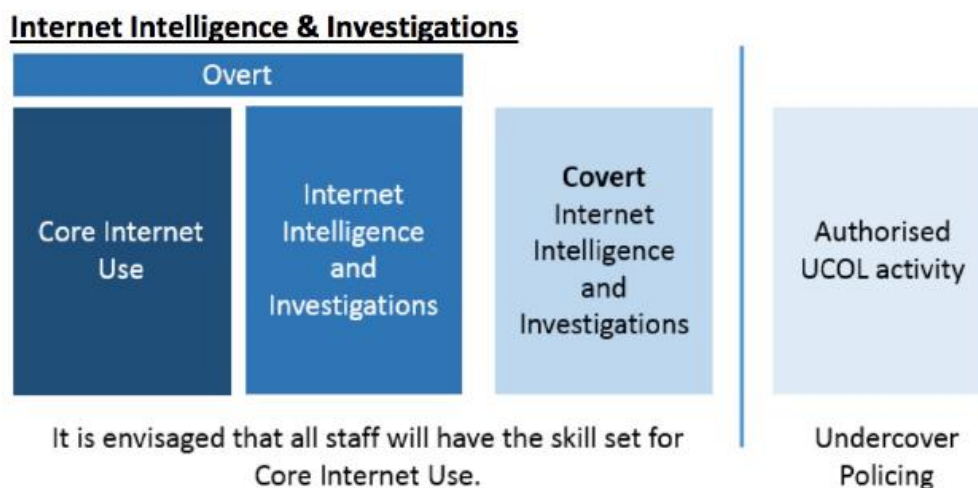
⁷⁷ <https://www.legislation.gov.uk/ukpga/2016/25/enacted>

⁷⁸ Covert Surveillance and Property Interference Revised Code of Practice, August 2018

An authorisation may be granted only where the Authorising Officer believes that the authorisation is necessary in the circumstances of the particular case: For the purpose of preventing and detecting crime and disorder”.⁷⁹

Vanaf 2015 zijn er landelijke, maar later ook lokale richtlijnen ontwikkeld door de *National Open Source Intelligence Working Group* (en in 2019 herzien) die kaders en definities bieden voor het gebruik van *open sources* in het operationele politiewerk.

Zo komt in onderstaand landelijke model het belangrijkste onderscheid in online informatievergarings tot uitdrukking. Het model is namelijk onderverdeeld in openlijke (overt) en heimelijke (covert) activiteiten. Voor de *covert* activiteiten is de RIPA (part II) van toepassing, voor de *overt* activiteiten is dat niet het geval.



Overt activiteiten

Openlijke/overt activiteit is onderverdeeld in 'kernegebruik van het internet' en 'internetonderzoeken' om onderscheid te maken tussen ad-hoc internetgebruik en de meer gestructureerde, methodische benadering van internetonderzoek door daartoe opgeleide professionals.

Het laagste niveau van internetonderzoek ziet op ‘*Core Internet Use* (niveau 1): het openlijk internetonderzoekswerk zoals het doorzoeken van sociale mediasites en andere openlijke beschikbare websites. Voorbeelden zijn het controleren of een individu een social media account heeft en het bekijken van openbare profielen om bewijs of inlichtingen te verkrijgen. Kernegebruik van het internet wordt omschreven als ‘het openlijke en ad-hoc gebruik van online bronnen en zoekmachines om basisinformatie te verschaffen’.⁸⁰ Het belangrijkste onderscheidende kenmerk van onderzoek op dit niveau is dat politieagenten ‘geen toegang mogen hebben tot delen van het internet die een gebruikersnaam en wachtwoord vereisen’.⁸¹

Overt internet intelligence and investigations (niveau 2) wordt omschreven als ‘een gestructureerde, methodische, taakgerichte en geplande aanpak van online onderzoek, uitgevoerd door een passend getraind persoon.’ Voorbeelden van dergelijk internetonderzoek zijn het gebruik van openlijke profielen om in te loggen op en toegang te krijgen tot platforms, het gebruik van

⁷⁹ The Regulation of Investigatory Powers ACT (RIPA) Policy and Procedure, Lancaster City Council.

⁸⁰ NPCC, Internet Intelligence & Investigations Strategy 2019.

⁸¹ Idem.

geavanceerde zoektechnieken om systematisch en gericht onderzoek uit te voeren, het monitoren van online activiteiten met betrekking tot vooraf geplande of spontane gebeurtenissen.

In de *guideline* van de *Investigatory Powers Commissioner's office*, de autoriteit die is aangewezen om toezicht te houden op organisaties met *investigatory powers* wordt het gebruik van 'overt' social media monitoring als volgt gedefinieerd:

The Surveillance Commissioner's Guidance defines overt social media monitoring as looking at 'open source' data, being publicly available data and data where privacy settings are available but not applied. However, to be 'overt' it must also involve only a 'one-off' look at the individual's social media. If this becomes 'repeated viewing', even of so-called open source sites, then this becomes 'covert' social media monitoring.

Voor overt activiteiten mogen geen heimelijke tactieken worden gebruikt en wanneer een gebruikersnaam en wachtwoord vereist zijn om toegang te krijgen tot een online ruimte, moeten de referenties aangeven dat het account of profiel wordt gebruikt voor politiedoeleinden en moet een record van alle activiteiten worden bijgehouden. Systematische monitoring van een persoonlijk profiel (zelfs wanneer deze openbaar is en een politieaccount wordt gebruikt), wordt beschouwd als een activiteit die zou vallen binnen het heimelijke inlichtingen- en onderzoekswerk dat valt onder RIPA, waarvoor aparte toestemming vereist is en waarbij de noodzakelijkheid en evenredigheid worden gewogen. Dus wanneer er sprake is van *repeated viewing* is *Regulation of Investigatory Powers Act 2000* van toepassing en zijn alle waarborgen en vereisten rondom autorisatie/toestemming die deze wet voorschrijven van toepassing. In dit geval is er sprake van *covert monitoring*.

Covert activiteiten

Niveaus 3 en 4 verwijzen naar (covert) heimelijk internetonderzoek, namelijk wanneer het onderzochte individu niet op de hoogte is van het feit dat hij online wordt gevolgd. Voorbeeld hiervan is het gebruik van nepprofielen om in te loggen op sociale mediasites. Op dit niveau van onderzoek mag echter geen interactie zijn met de betrokkene, geen vrienden maken, berichten achterlaten of deelnemen aan groepen. Internetonderzoek moet op deze niveaus plaatsvinden op beveiligde computers die niet naar de politie te herleiden zijn. Alle informatie die op level 2 en 3 is verzameld moet worden vastgelegd in de politiesystemen en alle nepprofielen moeten worden geregistreerd. Op het zwaarste niveau van onderzoek is sprake van *undercoverwork* waarvoor nog strengere eisen en voorwaarden uit de RIPA gelden.⁸²

Privacywaarborgen

De *Human Rights Act 1998* speelt een belangrijke rol in het reguleren en beperken van de manier waarop overheidsinstanties, waaronder de politie, online informatie vergaren en gebruiken om de openbare orde te handhaven. Deze wet is een afgeleide van het Europees Verdrag voor de Rechten van de Mens (EVRM) en legt beperkingen op aan de overheid om de rechten en vrijheden van individuen te waarborgen. Artikel 8 van het EVRM, dat is opgenomen in de Human Rights Act erkent het recht op respect voor privéleven en familie. Het vereist dat overheidsinstanties, inclusief de politie, zich onthouden van ongerechtvaardigde inmenging in het privéleven van individuen.

⁸² Elena M. Egawhary, *The Surveillance Dimensions of the Use of Social Media by UK Police Forces*, *Surveillance & Society*, 2019.

De *Data Protection Act 2018* is afgeleid van de Algemene Verordening Gegevensbescherming en EU-richtlijn 2016/680 en is de algemene gegevensbeschermingswet in het Verenigd Koninkrijk. De wet bevat bepalingen ter bescherming van persoonsgegevens. Part 3 van de wet bevat bepalingen die specifiek gelden voor het verwerken van persoonsgegevens door *law enforcement authorities*.⁸³ De politie moet voldoen aan de principes van gegevensbescherming, waaronder het rechtmatig, eerlijk en transparant verwerken van persoonsgegevens.

Zowel de covert als overt activiteiten moeten voldoen aan de eisen en waarborgen die worden gesteld door de Human Rights act en de Data Protection Act 2018.

De *Investigatory Powers Act 2016* bevat verschillende waarborgen om de privacy van inwoners te beschermen. Deze waarborgen zijn bedoeld om ervoor te zorgen dat de bevoegdheden van de wet op een evenwichtige en proportionele manier worden toegepast. Zo moet het uitoefenen van de bevoegdheden op grond van de *IPA* voldoen aan de beginselen van noodzakelijkheid en proportionaliteit. Dit betekent dat de inbreuk op de privacy gerechtvaardigd moet zijn door een noodzaak en dat deze in verhouding moet staan tot het beoogde doel.

Voor bepaalde zware (covert) bevoegdheden is rechterlijke toestemming vereist. Een rechter moet beoordelen of het verzamelen van bepaalde gegevens noodzakelijk en proportioneel is voor de beoogde doeleinden. Verder bevat de *IPA* bepalingen ter bescherming van de privacy van communicatiegegevens. Het ongeoorloofd onderscheppen, verkrijgen, bekijken of openbaar maken van communicatiegegevens wordt als strafbaar beschouwd. Ook vereist de wet dat de overheidsinstanties transparant zijn over het gebruik van de bevoegdheden en periodiek rapporteren aan het parlement en de *Investigatory Powers Commissioner (IPC)*. Tot slot bevat de *IPA* specifieke bepalingen met betrekking tot het bewaren van gegevens, waarbij richtlijnen worden vastgesteld voor hoelang bepaalde soorten gegevens mogen worden bewaard.

De *IPA* voorziet verder in onafhankelijk toezicht op het gebruik van de bevoegdheden die de wet verleent. Dat toezicht wordt uitgeoefend door de *IPC*, die verantwoordelijk is voor het toezicht op het gebruik van bevoegdheden uit de *IPA*. De *IPC* heeft de bevoegdheid om onderzoeken uit te voeren en rapporten uit te brengen over het gebruik van de bevoegdheden.

Uit onderzoek van *Privacy International* dat onderzoek deed naar *overt social media monitoring* door de politie in Groot-Brittannië blijkt dat de privacy van burgers onvoldoende gewaarborgd wordt. Uit het onderzoek komt naar voren dat *a significant number of local authorities* (waaronder de politie) gebruik maakt van *overt social media monitoring*, als onderdeel van hun *intelligence gathering*. Deze praktijk komt veel meer voor dan de wettelijk gereguleerde inzet van *covert social media monitoring*, maar zonder dat daar altijd goede *guidelines* voor zijn opgesteld. Uit het onderzoek blijkt verder dat er weinig tot geen controles of audits worden uitgevoerd op de effectiviteit van dit type informatieverzameling en dat er doorgaans geen verantwoording wordt afgelegd over de wijze hoe het onderzoek wordt uitgevoerd, waarom het wordt uitgevoerd en wat er met de gegevens wordt gedaan. Indien je als burger je privacysettings niet zodanig hebt ingesteld dat informatie is afgeschermd, wordt alle toegankelijke informatie door de overheid als *open source* beschouwd.⁸⁴

⁸³ <https://ico.org.uk/for-organisations/law-enforcement/>

⁸⁴ Privacy International, *Is your Local Authority looking at your Facebook likes?* 2020.

3.3 De uitvoering van online informatievergaring

Binnen lokale politiediensten kunnen verschillende eenheden zich bezighouden met online informatievergaring bij het handhaven van de openbare orde. De naamgeving en organisatie van die eenheden variëren per politiekorps. Zo zijn er op regionaal niveau bijvoorbeeld *Intelligence Units*, dit zijn inlichtingeneenheden binnen de politie die belast zijn met het verzamelen, analyseren en interpreteren van informatie. Dit omvat vaak online bronnen waar potentiële bedreigingen van de openbare orde kunnen worden geïdentificeerd. Ook zijn er zogenoemde *Online Safety Units* die betrokken zijn bij het monitoren van sociale media en andere online platforms om dreigingen of verstoringen van de openbare orde te identificeren. Online informatievergaring gebeurt dus veelal op lokaal niveau.

Een belangrijke gebeurtenis die van grote invloed is geweest op ontwikkelingen rondom online informatie vergaren, waren de *London Riots* van 2011 waarbij grootschalige rellen plaatsvonden, eerst in Londen en later ook in andere Britse steden. Tijdens die gebeurtenissen werd duidelijk welk aanjagend effect sociale media kunnen hebben op openbare ordeverstoringen en welk potentieel het monitoren ervan kan hebben om dergelijke situaties in de toekomst te beheersen en voorkomen. De ontwikkelingen in het gebruik van sociale media door de politie hebben sindsdien een enorme vlucht genomen.

Het gebruik van sociale media door de politie valt grofweg uiteen in twee categorieën: communicatie en operationeel gebruik. De wijze waarop de politie met deze twee activiteiten omgaat kan erg verschillen per politieregio. Elke regio heeft een eigen handelingskader waarin het gebruik van online informatie wordt genormeerd. Er zijn echter landelijke kaders ontwikkeld die voor alle politieregio's gelden.⁸⁵

3.4 Toezicht

De *Information Commissioner's Office (ICO)* is de toezichthouder op gegevensbescherming en kan ingrijpen als er zorgen zijn over de naleving van de Data Protection Act 2018.

De *Investigatory Powers Commissioner's Office (IPCO)* is het onafhankelijke toezichthoudende orgaan in het Verenigd Koninkrijk dat toezicht houdt op het gebruik van onderzoeksbevoegdheden door politiediensten, inlichtingendiensten en andere overheidsinstanties. De IPCO werd opgericht in het kader van de *Investigatory Powers Act 2016 (IPA)*. De IPCO staat onder leiding van de *Investigatory Powers Commissioner*, doorgaans een voormalige rechter van het High Court of Court of Appeal. De organisatie bestaat uit een team van ervaren rechters (*Judicial Commissioners*), technische experts, auditors en juridisch personeel.⁸⁶

Voor het gebruik van de meest ingrijpende bevoegdheden – zoals het tappen van communicatie, hacken van apparaten (*equipment interference*) of bulk data-acquisitie – geldt dat een minister eerst toestemming moet geven op basis van noodzaak en proportionaliteit.⁸⁷ Deze toestemming wordt pas rechtsgeldig na goedkeuring door een *Judicial Commissioner* van de IPCO.

⁸⁵ Elena M. Egawhary, *The Surveillance Dimensions of the Use of Social Media by UK Police Forces*, *Surveillance & Society*, 2019.

⁸⁶ <https://www.ipco.org.uk/who-we-are/investigatory-powers-commissioner/>

⁸⁷ <https://www.ipco.org.uk/what-we-do/the-double-lock/>

De Judicial Commissioners beoordelen onafhankelijk of de aanvraag voldoet aan wettelijke eisen. Zij kunnen toestemming geven of weigeren, en bij twijfel aanvullende informatie opvragen.⁸⁸ Naast de voorafgaande toets voert de IPCO periodieke inspecties en audits uit bij politiediensten, inlichtingendiensten en andere bevoegde instanties. Daarbij wordt gekeken naar de rechtmatigheid en zorgvuldigheid van uitgevoerde handelingen, de dossiervorming, interne procedures en naleving van privacyregels. De bevindingen van de IPCO worden jaarlijks gerapporteerd in *annual reports*.⁸⁹

3.5 Inzet van technische hulpmiddelen

Cameratoezicht

In het Verenigd Koninkrijk worden technische hulpmiddelen ingezet bij het handhaven van de openbare orde. Zo wordt er veelvuldig gebruik gemaakt van cameratoezicht. Dit kan zowel fysiek cameratoezicht op straat als online surveillancecamera's omvatten. Cameratoezicht wordt gebruikt in verschillende openbare ruimtes, zoals stadscentra, winkelgebieden, transportknooppunten, en bij grote evenementen. De camera's worden bijvoorbeeld gebruikt om openbare evenementen te kunnen monitoren en om mogelijke problemen te identificeren.

Automatische nummerplaatherkenning (ANPR)

Ook ANPR naast opsporing van voertuigen onder omstandigheden ook gebruikt om de openbare orde te handhaven. Dit gebeurt bijvoorbeeld tijdens grootschalige evenementen, demonstraties of in gebieden waar er bezorgdheid is over de openbare veiligheid.

3.5.1 Toezicht op technische hulpmiddelen

Het gebruik van cameratoezicht en ANPR is onderworpen aan wet- en regelgeving om de privacy van individuen te waarborgen. Er zijn richtlijnen, zoals de Surveillance Camera Code of Practice, die politie en andere organisaties die cameratoezicht uitvoeren, moeten volgen. De Surveillance Camera Commissioner houdt toezicht op het gebruik van surveillancesystemen, waaronder Automatic Number Plate Recognition (ANPR). De Surveillance Camera Commissioner (SCC) is een onafhankelijke functionaris die is aangesteld om toezicht te houden op het gebruik van cameratoezicht en ervoor te zorgen dat dit gebeurt in overeenstemming met de wet en ethische normen.

⁸⁸ <https://www.ipco.org.uk/who-we-are/judicial-commissioners/>

⁸⁹ <https://www.ipco.org.uk/publications/annual-reports/>

4. Duitsland, deelstaat Hessen

4.1 Organisatie van de openbare ordehandhaving

De Bondsrepubliek Duitsland bestaat uit zestien deelstaten (Länder), allen met een eigen politiekorps (Länderpolizei). Artikel 30 van de Duitse grondwet bepaalt:

“De uitoefening van overheidsbevoegdheden en de vervulling van overheidstaken is de verantwoordelijkheid van de deelstaten, voor zover de Grondwet geen andere regeling bevat of toestaat.”

Historisch gezien zijn het doorgaans uitsluitend de deelstaten geweest die verantwoordelijk zijn voor het handhaven van de orde, met uitzondering van de periode tussen 1939 en 1945, waarin een gecentraliseerde politiemacht controle uitoefende. Als zodanig bestaat er slechts een relatief kleine federale politiemacht (Bundespolizei), die ondergeschikt is aan het Federale Ministerie van Binnenlandse Zaken. Haar taken draaien voornamelijk om grensbeveiliging, terrorismebestrijding en de bescherming van federale gebouwen.⁹⁰

In de Duitse deelstaat Hessen is de handhaving van de openbare orde primair de verantwoordelijkheid van de Landespolizei, die onder het Hessisches Ministerium des Innern und für Sport valt. Dit ministerie bepaalt het beleid en de operationele richtlijnen voor de politie in de deelstaat. De politie heeft de taak om de openbare veiligheid en orde te handhaven, potentiële bedreigingen te identificeren en aan te pakken, en om te reageren op incidenten en noodsituaties.

Daarnaast hebben lokale overheden, zoals gemeenten en steden, bevoegdheden om regels en verordeningen vast te stellen die specifiek gericht zijn op het handhaven van de openbare orde binnen hun grenzen. Ze kunnen bijvoorbeeld plaatselijke verordeningen aannemen die gedragingen zoals openbare dronkenschap, geluidsoverlast en de organisatie van evenementen reguleren.

⁹⁰ WRR, *Politiefunctie in een veranderende omgeving – Appendix D, Nordrhein-Westfalen*, 2021.

Deze lokale regelgeving moet wel binnen de kaders van de landelijke en deelstaatswetgeving vallen. In geval van ernstige openbare orde problemen kan de lokale politie ingrijpen en, indien nodig, ondersteuning krijgen van federale politiediensten.

Ter handhaving van de openbare orde in Hessen kan de politie feitelijke maatregelen zoals wegcontroles of surveillance nemen (art. 11 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung, HSOG). Deze maatregelen kunnen worden getroffen als er concreet gevaar dreigt voor de openbare orde en veiligheid. De wet geeft de politie de bevoegdheid noodzakelijke maatregelen te treffen om dreigende gevaren af te wenden en de openbare veiligheid te handhaven. Dit kan variëren van preventieve maatregelen tot direct ingrijpen bij incidenten die de openbare orde bedreigen.

Op grond van artikel 12 HSOG van de deelstaat Hessen kan de politie inlichtingen inwinnen door middel van een verhoor. Een persoon kan daartoe worden aangehouden. Hiertoe moet een concrete aanleiding bestaan, gebaseerd op feiten en omstandigheden. Bovendien moet de gevraagde informatie nodig zijn voor de handhaving van de openbare orde. Er mag ook geen sprake zijn van opsporing van strafbare feiten. De aanhouding wordt in de Duitse wetgeving aangemerkt als een tijdelijke inperking van de vrijheid. De te verhoren persoon kan zich beroepen op een verschoningsrecht. Op grond van artikel 14 HSOG kan de politie in het kader van de openbare orde handhaving persoonsgegevens inwinnen. Het gaat hierbij in het bijzonder om openbare manifestaties en samenscholingen. Uit feiten of omstandigheden moet blijken dat bij of in samenhang met de manifestatie of samenschooling de openbare orde zal worden verstoord of strafbare feiten zullen worden gepleegd. Het kan hier ook gaan om groepsgewijze verstoring van de openbare orde.^{91 92}

4.2 Het wettelijk kader voor de uitoefening van de openbare ordetaak

Openbare ordewetgeving

In Hessen zijn de bevoegdheden van de politie met betrekking tot surveillance op internet geregeld door verschillende wetten en voorschriften op federaal- en deelstaatsniveau.

Federale wetgeving

De Duitse Grondwet (Grundgesetz) beschermt de fundamentele rechten van individuen, zoals het recht op privacy dat is vastgelegd in artikel 2, paragraaf 1 en luidt als volgt:

Artikel 2 - Persoonlijke vrijheid

(1) Ieder heeft het recht op de vrije ontwikkeling van zijn persoonlijkheid, voor zover hij geen inbreuk maakt op de rechten van anderen en niet in strijd handelt met de grondwettelijke orde of de zeden.

In artikel 10 van de Grondwet wordt het brief-, post- en telecommunicatiegeheim beschermd:

Artikel 10 - Briefgeheim, postgeheim, telefoon- en telegraafgeheim

(1) Het briefgeheim, het postgeheim, het telefoon- en telegraafgeheim zijn onschendbaar.

(2) Inbreuken hierop zijn slechts toegestaan op grond van een wet.

⁹¹ Rogier, L.J.J. e.a. *Handhaving van de openbare orde in het buitenland: overzicht van bevoegdheden, praktische toepassing en toepasbaarheid in Nederland*, 2002, p.22.

⁹² <https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-SOGHEV14IVZ>

Dit artikel waarborgt de onschendbaarheid van communicatie en stelt dat inbreuken hierop alleen mogelijk zijn op basis van een wet.

Ter uitwerking van de AVG en EU-richtlijn 2016/680 regelt de federale Bundesdatenschutzgesetz (BDSG), de federale wet op gegevensbescherming, de verwerking van persoonsgegevens door overheidsinstanties en particuliere organisaties in Duitsland, inclusief bepalingen met betrekking tot de bevoegdheden van de politie om persoonsgegevens te verzamelen en te gebruiken, waaronder die welke via internet worden verkregen.

Op federaal niveau functioneert daarnaast het Telekommunikationsgesetz (TKG) dat de telecommunicatiesector in Duitsland regelt en bepalingen over de bescherming van persoonsgegevens en communicatiegeheimen bevat. De wet voorziet in uitzonderingen op het telecommunicatiegeheim voor rechtshandhaving en nationale veiligheid, maar deze moeten in overeenstemming zijn met de Grondwet en andere toepasselijke wetten.

Naast het Telekommunikationsgesetz (TKG), bestaat op federaal niveau een wet die toezicht op telecommunicatie en andere geheime onderzoeksmaatregelen reguleert, het Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, aangeduid als G10. De wet regelt de bevoegdheden van de Duitse inlichtingendiensten en de politie, inclusief surveillance en monitoring van communicatie, waaronder internetcommunicatie, voor doeleinden van nationale veiligheid. De G10-wet regelt specifiek het toezicht op telecommunicatie op het gebied van strategische telecommunicatie-inlichtingen, met name bij het verzamelen van gegevens die over grensoverschrijdende communicatienetwerken stromen. De G10-wet geeft autoriteiten toestemming om toezicht te houden op telecommunicatie om de interne veiligheid en andere belangrijke zaken van de staat te beschermen. Dit omvat onder meer de bestrijding van terrorisme, spionage en andere ernstige misdrijven. Surveillance onder de G10-wet is alleen onder bepaalde voorwaarden toegestaan. Hierbij valt bijvoorbeeld te denken aan de goedkeuring van een onafhankelijk orgaan (de zogenaamde G10 Commissie) en het vaststellen van een specifiek toezichtdoel dat in het algemeen belang is. De G10-wet bevat bepalingen die bedoeld zijn om ervoor te zorgen dat de fundamentele rechten van de betrokkenen, in het bijzonder het recht op informatieve zelfbeschikking en telecommunicatiegeheim, worden gewaarborgd. Deze omvatten bijvoorbeeld vereisten voor proportionaliteit en data-economie bij het uitvoeren van toezichtmaatregelen. De wet vereist dat toezichtmaatregelen door de autoriteiten regelmatig worden herzien en gecontroleerd om ervoor te zorgen dat ze wettig en proportioneel zijn. Bovendien wordt een zekere mate van transparantie gewaarborgd door verslaglegging aan het parlement over de uitvoering van toezichtmaatregelen. De G10-wet is verschillende keren gewijzigd om de technologische ontwikkelingen en wettelijke vereisten weer te geven. Het is een belangrijk onderdeel van het Duitse rechtssysteem op het gebied van toezicht en geheime onderzoeksmaatregelen.

Regeling op Landsniveau

Naast deze wettelijke regelingen op federaal niveau is er in de deelstaat Hessen wetgeving gericht tot de politie. Het HSOG. In deze wet staat ook een specifieke regeling voor geautomatiseerde verwerking van persoonsgegevens met het oog op de openbare veiligheid en orde. Het gaat hierbij dus om gegevens in bestanden die reeds bij de politie aanwezig zijn (het gaat niet specifiek over online onderzoek):

§ 25a HSOG – Automatisierte Anwendung zur Datenanalyse

(1) Die Polizeibehörden können in begründeten Einzelfällen gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse weiterverarbeiten zur vorbeugenden Bekämpfung von in § 100a Abs.

2 der Strafprozessordnung genannten Straftaten oder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind.

In een uitspraak van [16 februari 2023](#)⁹³ verklaarde het Bundesverfassungsgericht in Karlsruhe deze bepaling van het HSOG in de deelstaat Hessen waarin de politie de bevoegdheid had gekregen persoonsgegevens met behulp van grootschalige geautomatiseerde verwerking te analyseren in strijd met onder meer artikel 2, lid 1 van de Grondwet (informatieele zelfbeschikking). Daarvoor gebruikte de politie een systeem van het Amerikaanse bedrijf Palantir, onder de naam hessenDATA. Deze software werd sinds 2017 in Hessen gebruikt, jaarlijks duizenden keren. Het Bundesverfassungsgericht verbood het gebruik van Palantir niet zonder meer, maar oordeelde wel dat de regels veel strikter moeten worden geformuleerd, en dat het platform alleen mag worden ingezet bij concreet gevaar. Het hof oordeelde dat de regels te breed zijn geformuleerd, zowel op het vlak van de verwerking van data als op het vlak van de methodes die de politie mag inzetten. Momenteel ligt de lat voor de inzet van het systeem veel te laag, aldus het grondwettelijk hof. [Artikel 25a HSOG](#)⁹⁴ is per 12 juli 2023 naar aanleiding van de uitspraak van het grondwettelijk hof aangepast. Het eerste lid luidt nu als volgt:

- (1) Die Polizeibehörden dürfen rechtmäßig gespeicherte personenbezogene Daten auf einer Analyseplattform automatisiert zusammenführen. Sie dürfen nach Maßgabe der Sätze 3 bis 6 und der Abs. 2 bis 5 diese zusammengeführten Daten, auch gemeinsam mit weiteren rechtmäßig erhobenen personenbezogenen Daten, verknüpfen, aufbereiten und auswerten sowie für statistische Zwecke anwenden (automatisierte Anwendung zur Datenanalyse). Die automatisierte Anwendung zur Datenanalyse ist ein technisches Hilfsmittel, das es den Polizeibehörden bei der Erfüllung ihrer Aufgaben nach Maßgabe der folgenden Absätze ermöglichen soll, ihre Bewertungen, Prognosen und Entscheidungen auf der Grundlage möglichst verlässlicher Tatsachenfeststellungen zu treffen. Sie erfolgt immer anhand anlassbezogener und zielgerichteter Suchkriterien. Sie wird manuell ausgelöst und läuft regelbasiert auf einer von Menschen definierten Abfolge von Analyse- und Verarbeitungsschritten ab. Eine direkte Anbindung an Internetdienste ist ausgeschlossen.

Deze zaak ging niet over online onderzoek, maar over geautomatiseerde gegevensanalyse. De uitspraak is relevant vanwege het feit dat hieruit blijkt dat dergelijke bepalingen getoetst worden aan de grondwet en dat een beperking een grondslag moet hebben in een wet (in formele zin) en dat die grondslag zo specifiek mogelijk moet zijn geformuleerd. Dat is ook relevant voor het doen van online onderzoek en hoe dit in wetgeving moet zijn vastgelegd.

Bevoegdheden om online informatie te vergaren met het oog op openbare orde-handhaving

De Duitse politie heeft bevoegdheden om het internet te surveilleren. Dit omvat onder meer het verzamelen van informatie van openbare en deels openbare bronnen op het internet. Daarbij gaat het om het gebruik van informatie die vrij toegankelijk is op het internet, zoals sociale media posts, forums, en andere openbare digitale platforms. Voor het uitvoeren van diepgaandere online surveillanceactiviteiten, zoals het onderscheppen van privé communica-

⁹³ ECLI:DE:BVerfG:2023:rs20230216.1bvr154719.

⁹⁴ https://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?t=171128020382263565&xid=169564,130.

tie, is een gerechtelijk bevel nodig. Deze bevoegdheden zijn geregeld in verschillende wetten, waaronder het Bundeskriminalamtgesetz (BKA-Gesetz), dat het Bundeskriminalamt (BKA) bevoegdheden geeft voor activiteiten zoals het monitoren van online communicatie in specifieke gevallen.

Een belangrijk principe en regelmatig terugkerende eis van de Duitse politie betreft het verkrijgen van gelijke juridische bevoegdheden in zowel de fysieke als de digitale wereld. Dit houdt in dat de huidige wetgeving met betrekking tot bevoegdheden in de digitale sfeer moet worden uitgebreid om overeen te komen met de fysieke bevoegdheden, zoals bijvoorbeeld het aftappen van communicatie via berichtendiensten of online doorzoeken van apparaten.

De Duitse politiediensten voeren sinds de jaren negentig ook regelmatig 'online patrouilles' uit (virtuelle Streifenfahrten; anlassunabhängige Recherche im Internet), waarbij ze bijvoorbeeld sociale mediaplatforms zoals Facebook doorzoeken. Dergelijke online patrouilles schenden geen wettelijke rechten en zijn goed vergelijkbaar met patrouilles in de fysieke wereld.

Zodra echter bepaalde grenzen worden overschreden, zoals toegang verkrijgen tot een besloten groep met een dekmantelverhaal of het opslaan van specifieke persoonlijke gegevens, ontstaat er een juridische discussie over de toelaatbaarheid daarvan.⁹⁵

Privacywaarborgen

De Bundesdatenschutzgesetz (Duitse Wet Bescherming Persoonsgegevens) legt de bescherming tegen misbruik van persoonsgegevens vast in Duitsland. Op het niveau van het Land Hessen geldt het Hessisches Datenschutzgesetz (HDSG). De Landesdatenschutz-beauftragte (Commissaris voor Gegevensbescherming) in Hessen houdt toezicht op de naleving van deze wet.

4.3 De uitvoering van online informatievergaring

Inzet van online onderzoeken

Voor het surveilleren in open bronnen heeft de Duitse politie geen afzonderlijke toestemming nodig. Wanneer het gaat om surveilleren in besloten groepen op het internet heeft de politie een gerechtelijk bevel nodig. Een dergelijk bevel wordt verkregen wanneer er redelijke verdenkingen zijn van criminele activiteiten. Of de surveillance gerechtvaardigd is, wordt beoordeeld op basis van de beschikbare bewijzen en de ernst van de vermoede misdrijven.

Er leeft in Duitsland een discussie over de grens tussen openbare en niet openbare bronnen. Zo is het onduidelijk of een chat- of facebookgroepen moet worden gezien als open of gesloten wanneer de politie beschikt over een uitnodigingslink of is toegelaten tot een bepaalde niet openbare groep. Hoe de politie hier mee omgaat, verschilt volgens een gesprekspartner per deelstaat. Dit hangt af van interne richtlijnen die per deelstaat verschillen. Hoewel niet bekend met de inhoud geeft een gesprekspartner wel aan dat de deelstaat Berlijn hierover interne regels heeft opgesteld. De inhoud is hem en ons echter onbekend.

⁹⁵ WRR, Appendix D, North Rhine-Westphalia/Germany, p.10-11.

4.4 Toezicht

Of er sprake is van een (te grote) inbreuk op de privacy, is in beginsel aan de rechter om te beoordelen. Volgens gesprekspartners worden in de praktijk echter nauwelijks klachten ingediend, mede omdat burgers vaak niet weten dat hun gegevens zijn geanalyseerd. Er ontbreekt volgens gesprekspartners transparantie over de inzet van online middelen, wat toezicht en publieke verantwoording verder bemoeilijkt.

Er zijn binnen de politiediensten interne functionarissen voor gegevensbescherming, die toezien op de naleving van privacyregels. Daarnaast bestaan er externe toezichthouders op gegevensbescherming, zowel op federaal niveau (zoals de Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI) als op Länder-niveau (bijvoorbeeld de Hessische Beauftragte für Datenschutz und Informationsfreiheit). Deze autoriteiten zijn formeel onafhankelijk, maar beschikken volgens gesprekspartners vaak over beperkte personele en financiële middelen. Daardoor is het effectieve toezicht op online gegevensverzameling door de politie in de praktijk beperkt.

4.5 Inzet van technische hulpmiddelen

Cameratoezicht

In Hessen is het gebruik van cameratoezicht gereguleerd door het Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) en het Hessisches Datenschutzgesetz (HDSG), die samenhangen met de algemene Duitse en Europese privacywetgeving zoals de Algemene Verordening Gegevensbescherming (AVG). Cameratoezicht door de politie en andere autoriteiten moet worden gerechtvaardigd door specifieke veiligheidsbehoeften en moet proportioneel zijn aan het nagestreefde doel.

Het plaatsen van camera's in openbare ruimtes vereist een gerechtelijk bevel of een specifieke wetgevingshandeling, afhankelijk van de situatie en de locatie van de camera's. Daarnaast moeten burgers duidelijk geïnformeerd worden over het gebruik van camera's in hun omgeving door middel van zichtbare borden of andere notificaties. Dit is om te voldoen aan de transparantievereisten die worden gesteld door de privacywetgeving.

Voor het gebruik van cameratoezicht in meer private settings, zoals in bedrijven of voor persoonlijke beveiliging, moeten eigenaren ook voldoen aan de AVG-vereisten, die onder meer inhouden dat de inbreuk op de privacy geminimaliseerd wordt en dat de gegevensbescherming van de gefilmde personen gewaarborgd is.

Automatische nummerplaatherkenning (ANPR)

Op [18 december 2018](#)⁹⁶ verklaarde het grondwettelijk hof in Karlsruhe de eerdere regeling voor het geautomatiseerd uitlezen van kentekens in Sectie 14a HSOG grotendeels ongrondwettelijk. [Sectie 14a HSOG](#)⁹⁷ is daarom gewijzigd, rekening houdend met deze uitspraak. In de gewijzigde versie is het automatisch vastleggen van beelden van voertuigen en het vastleggen van hun kentekenplaten en de daaropvolgende vergelijking met politie-informatiesystemen

⁹⁶ ECLI:DE:BVerfG:2018:rs20181218.1bvr279509.

⁹⁷ https://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?t=144281760418936044&xid=169564,120.

gebaseerd op redenen die dienen ter bescherming van juridische belangen van op zijn minst aanzienlijk gewicht of een ander vergelijkbaar zwaar openbaar belang. Bovendien wordt een duidelijke beperking tot plaatsen met een grensverbinding vastgelegd, zoals vereist door het grondwettelijk hof. Een ingevoegde paragraaf 1a van artikel 14 a HSOG regelt de bescherming van de persoonlijke rechten van mensen die zich buiten het geregistreerde voertuig bevinden. Onder de daar gespecificeerde voorwaarden is het mogelijk om systemen voor het automatisch uitlezen van kentekens in voertuigen te gebruiken tijdens politiepatrouilles.

Toezicht op technische hulpmiddelen

Het toezicht op de inzet van technische hulpmiddelen wordt uitgevoerd door verschillende instanties, waaronder de Hessische Datenschutzbeauftragte (de privacytoezichthouder van Hessen) die controleert of de privacyregels worden nageleefd. Daarnaast moeten operationele procedures en het gebruik van verzamelde gegevens regelmatig worden geëvalueerd om de naleving van de wet te garanderen. Bovendien is er vaak een gerechtelijk bevel vereist om toestemming te geven voor het gebruik van dergelijke surveillancetechnologieën in specifieke gevallen, vooral wanneer dit ingrijpt in de persoonlijke levenssfeer.

5. België

5.1 Organisatie van de openbare ordehandhaving

In België is de burgemeester primair verantwoordelijk voor de lokale openbare orde.⁹⁸ Als de burgemeester zijn bevoegdheden – al dan niet vrijwillig – niet nakomt, de verstoring van de openbare orde zich uitstrekt over verschillende gemeenten, of het algemeen belang dit vereist, kunnen de provinciegouverneur of de minister van Binnenlandse Zaken de bevoegdheid voor het handhaven van de openbare orde op zich nemen.⁹⁹

Voor het bewaren of herstellen van de openbare orde is de burgemeester onder meer de verantwoordelijke overheid inzake de *bestuurlijke politie* op het grondgebied van de gemeente.¹⁰⁰

Organisatie van de Belgische politie

In België is de politie georganiseerd op twee niveaus: de federale politie en de lokale politie.¹⁰¹ Deze twee niveaus samen heten de geïntegreerde politie.¹⁰² Daarnaast wordt onderscheid gemaakt tussen de bestuurlijke politie (onder het gezag van de minister van Binnenlandse zaken) en de gerechtelijke politie (onder het gezag van de minister van Justitie).

Zowel de bestuurlijke politie¹⁰³ als de gerechtelijke politie¹⁰⁴ dragen bij tot de handhaving van de openbare orde. Zelfs als ze in de praktijk soms door elkaar lopen, is het van belang de bestuurlijke en gerechtelijke politie van elkaar te onderscheiden, omdat de opdrachten, de bevoegdheden en de verantwoordelijke overheden – zoals hiervoor reeds is weergegeven – van elkaar verschillen. Het criterium dat de bestuurlijke politie onderscheidt van de gerechtelijke politie is de concrete finaliteit van het optreden. In de meeste gevallen, en

⁹⁸ <https://repub.eur.nl/pub/1119/CLD005.pdf>, p. 63. De verantwoordelijkheid van de burgemeester voor handhaving van openbare orde is niet expliciet vastgelegd in de Nieuwe Gemeentewet, zie ook https://libstore.ugent.be/fulltxt/RUG01/002/479/379/RUG01-002479379_2018_0001_AC.pdf, p. 35.

⁹⁹ Art 11 lid 1 Wet op het politieambt.

¹⁰⁰ Artikel 133 nieuwe gemeentewet.

¹⁰¹ Zie ook WRR, Politiefunctie in een veranderende omgeving, Appendix C – België, p. 6.

¹⁰² De inrichting van de politieorganisatie is vastgelegd in de Wet tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.

¹⁰³ Artikel 14 Wet op het politieambt https://www.ejustice.just.fgov.be/cgi_loi/change_lg_2.pl?language=nl&nm=1992000606&la=N

¹⁰⁴ Artikel 15 Wet op het politieambt.

zeer zeker bij een noodsituatie of wanneer er sprake is van samenloop van zware ordeverstoring en ernstige strafbare feiten, wordt prioriteit gegeven aan de bestuurlijke politie en daarmee aan de hulpverlening, aan de bescherming van personen en aan de handhaving en het herstel van de openbare orde. Het optreden van de gerechtelijke politie vindt plaats nadat de orde voldoende is hersteld.¹⁰⁵ De gerechtelijke politie is onder meer belast met de opsporing van misdrijven en het verzamelen van bewijs.

Benadrukt wordt dat het optreden van de bestuurlijke politie bovenal een preventief karakter heeft, waarbij het met name gaat om door middel van preventieve maatregelen verstoringen van de openbare orde te voorkomen om vervolgens, indien de openbare orde toch verstoord wordt, handhavend op te treden.¹⁰⁶

De lokale politie omvat 196 politiezones. Er bestaan twee soorten politiezones, namelijk eengemeentepolitiezones en meergemeentepolitiezones. Bij eengemeentepolitiezones is het grondgebied gelijk aan die van de gemeente. Bij meerpolitiezones worden de taken van de raad uitgevoerd door de politieraad en de taken van de burgemeester door het politiecollege. Het politiecollege bestaat uit burgemeesters van gemeenten waar de politiezone uit bestaat. Het politiekorps wordt aangestuurd door een korpschef, die vervolgens onder het gezag van de burgemeester of – bij meerpolitiezones – onder het gezag van het politiecollege staat. Voor zover het gaat om justitiële taken (uitgevoerd door de gerechtelijke politie) staat de politie onder het gezag van de procureur des konings of de onderzoeksrechter.

5.2 Het wettelijk kader voor de uitoefening van de openbare ordetaak

Er is in België weinig geregeld als het gaat om bevoegdheden voor het doen van online onderzoek door de politie bij het handhaven van de openbare orde. België kent niet een wet op de openbare orde waarin bevoegdheden aan de politie zijn toegekend ter handhaving van de openbare orde.¹⁰⁷ Bevoegdheden voor de politie zijn voor een belangrijk deel geregeld in de Wet op het politieambt (Wpa), maar die hebben betrekking op de fysieke wereld. Hierna bespreken we op hoofdlijnen het wettelijk kader voor de uitvoering van de openbare ordetaak (de Nieuwe Gemeentewet) en de bevoegdheden voor de politie voor het doen van online onderzoek bij het handhaven daarvan (Wpa). Voor het verwerken van persoonsgegevens is de Belgische uitvoeringswet van de AVG en EU-richtlijn 2016/680 ten slotte relevant.

De Nieuwe Gemeentewet

Zoals gezegd rust de verantwoordelijkheid voor het handhaven van de openbare orde op het grondgebied van de gemeenten in de handen van de burgemeester.¹⁰⁸ Voor de uitvoering van de taken op het gebied van de openbare orde handhaving vormen artikel 133 tot en met 135 van de Nieuwe Gemeentewet de basis.

In artikel 133 Nieuwe Gemeentewet is bepaald dat de burgemeester is belast met de uitvoering van *‘de politiewetten, de politiedecreten, de politieordonnanties, de politieverordeningen*

¹⁰⁵ Zie ook ministerie van Binnenlandse Zaken, ministeriële omzendbrief OOP 41bis betreffende de operationalisering van het referentiekader CP 4bis over het genegotieerd beheer van de openbare ruimte van 30 januari 2025, par. 2.2.4.

¹⁰⁶ Art. 14 Wet op het politieambt.

¹⁰⁷ <https://zoek.officielebekendmakingen.nl/nds-bzk0300082-b1.pdf>, p.7.

¹⁰⁸ RvS 1 februari 1999, nr. 78466; https://libstore.ugent.be/fulltxt/RUG01/002/479/379/RUG01-002479379_2018_0001_AC.pdf, p. 37.

en de politiebepalingen. Ook is in dat artikel vastgelegd dat de burgemeester de verantwoordelijke overheid is inzake de bestuurlijke politie op het grondgebied van de gemeente.

Artikel 134 van de Nieuwe Gemeentewet regelt bevoegdheden die de burgemeester toekomt in het kader van de openbare orde. Zo kan de burgemeester op grond van artikel 134 quater in het geval de openbare orde rond een voor het publiek toegankelijke inrichting wordt verstoord door gedragingen in die inrichting, deze sluiten. Daarnaast kan de burgemeester op grond van artikel 134 sexies in geval van verstoring van de openbare orde veroorzaakt door onder meer individuele of collectieve gedragingen, en die een verstoring van de openbare orde of overlast met zich meebrengt, beslissen over te gaan tot een tijdelijk plaatsverbod (te vergelijken met het Nederlands gebiedsverbod).

De gemeenten hebben op grond van artikel 135 tot taak *'het voorzien, ten behoeve van de inwoners, in een goede politie, met name over de zindelijkheid, de gezondheid, de veiligheid en de rust op openbare wegen en plaatsen en in openbare gebouwen.'* Paragraaf 2 van artikel 135 regelt de gemeentelijke politiebevoegdheden. In het artikel worden zes politietaken genoemd. Ten aanzien van de openbare orde taak zijn de tweede en derde paragraaf van dit artikel het meest relevant:

2. het tegengaan van inbreuken op de openbare rust, zoals vechtpartijen en twisten met volksoptocht op straat, tumult verwekt in plaatsen van openbare vergadering, nachtgerecht en nachtelijke samenscholingen die de rust van de inwoners verstoren;
3. het handhaven van de orde op plaatsen waar veel mensen samenkomen, zoals op jaarmarkten en markten, bij openbare vermakelijkheden en plechtigheden, vertoningen en spelen, in drankgelegenheden, kerken en andere openbare plaatsen;

In de zevende paragraaf gaat het over de openbare overlast:

7. het nemen van de nodige maatregelen, inclusief politieverordeningen, voor het tegengaan van alle vormen van openbare overlast.

Openbare overlast is eigenlijk een lichtere vorm van de verstoring van de openbare orde volgens de Raad van State.¹⁰⁹ Het Grondwettelijk hof bevestigt dit standpunt en beschrijft openbare overlast als: *'lichtere vormen van verstoring van de openbare rust, de veiligheid, de gezondheid en de zindelijkheid die schadelijk of hinderlijk zijn en die de normale druk van het sociale leven overschrijden.'*¹¹⁰

De Wet op het politieambt

In België is er een juridische basis van algemene strekking voor het verzamelen van persoonsgegevens door de politie. Artikel 44/1 § 1 Wpa luidt: *'In het kader van de uitoefening van hun opdrachten, bedoeld in hoofdstuk III], afdeling 1, en overeenkomstig de doeleinden omschreven in artikel 27 van de wet gegevensbescherming kunnen de politiediensten informatie en persoonsgegevens verwerken voor zover deze laatste toereikend, terzake dienend en niet overmatig van aard zijn in het licht van de doeleinden van bestuurlijke en van gerechtelijke politie waarvoor ze verkregen worden en waarvoor ze later verwerkt worden.'* Hierbij moet de politie de beginselen voor het verwerken van gegevens uit de artikelen 28 tot en met 35 van de *Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* in acht nemen.

¹⁰⁹ RvS, arrest BVBA BELGIUM BUSINESS COMPANY, nr. 202.037 van 18 maart 2010.

¹¹⁰ G.H., nr. 44/2015, 23 april 2015, B. 19.6 en 10.

Daarnaast regelt artikel 26 het betreden van publieke plaatsen door de politie. Artikel 26 Wpa luidt: *‘De politieambtenaren kunnen steeds de voor publiek toegankelijke plaatsen alsook de verlaten onroerende goederen betreden teneinde toe te zien op de handhaving van de openbare orde en de naleving van de politiewetten en -verordeningen.’*

Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens

Dit is de Belgische uitvoeringswet van onder meer de AVG en de richtlijn (EU) 2016/680. De wet stelt grenzen aan wat mag worden verzameld en verwerkt, en onder welke voorwaarden. Bij het verwerken van persoonsgegevens door de politie moeten de beginselen van artikel 28 tot en met 35 in acht worden genomen.

Grondwet

Artikel 22 van de Belgische Grondwet bepaalt dat ieder recht heeft op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.

5.2.1 Mogelijkheden voor het doen van online onderzoek in België

Artikel 26 van de Wpa regelt dat politieambtenaren in het kader van hun algemene politiebevoegdheden voor publiek toegankelijke plaatsen, zoals een winkel of treinstation, kunnen ‘betreden’ voor het uitoefenen van opdrachten van de bestuurlijke en gerechtelijke politie.¹¹¹

Wetsvoorstel wijziging art. 26 Wpa

In 2015 werd er een wetsvoorstel ingediend om duidelijkheid te scheppen over het online surveilleren op publiek toegankelijke plaatsen op internet. Er werd een wijziging van artikel 26 Wpa voorgesteld om artikel 26 ook van toepassing te laten zijn op de virtuele wereld. Het voorstel was het volgende lid toe te voegen aan artikel 26:

‘Voor de toepassing van deze wet worden de voor het publiek toegankelijke plaatsen op het internet of op andere elektronische communicatienetwerken, ongeacht of er voor het nemen van de toegang daartoe bepaalde vormelijke toegangsformaliteiten moeten worden ondernomen, gelijkgesteld met publiek toegankelijke plaatsen. De politieambtenaren mogen deze plaatsen bezoeken, bestuderen en er kopieën van nemen.’

Met dit artikel zouden de voor publiek toegankelijke internetplaatsen gelijk worden gesteld aan fysiek publiek toegankelijke plaatsen en zouden politieagenten ook binnen de publieke virtuele wereld kunnen patrouilleren.¹¹² De Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) bracht naar aanleiding van het wetsvoorstel een advies uit. De CBPL was niet tegen het wetsvoorstel, maar vond dat het voorstel voor de wijziging van artikel 26 niet duidelijk genoeg was. De CBPL stelde daarom een amendement van de tekst voor. Het voorstel om artikel 26 te wijzigen is uiteindelijk niet ingevoerd.¹¹³

¹¹¹ R. Saelens, De wet op het politieambt en technologische ontwikkelingen: de focus op internet patrouilleren in het kader van de bestuurlijke politie, p.385, in De sluier rond anonimiteit opgelicht....

¹¹² https://libstore.ugent.be/fulltxt/RUG01/002/479/312/RUG01-002479312_2018_0001_AC.pdf

¹¹³ Zie ook opmerking 48 van de Commissie voor de bescherming van de persoonlijke levenssfeer, Advies over het voorontwerp van wet betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties (CO-A-2016-021), nr. 21/2016 van 18 mei 2016. Volgens Verhage en Vermeulen is er vooralsnog geen politieke consensus binnen de regering, zie p. 23 in Update in de Criminologie VIII Mensenrechten en opsporing, terrorisme en migratie - Update in de Criminologie, 2017.

Ondanks dat artikel 26 Wpa niet is aangepast, moet de bepaling volgens sommige auteurs wel van toepassing worden beschouwd op digitaal publiek toegankelijk plaatsen.¹¹⁴ Ter onderbouwing hiervan kan worden gewezen op een arrest van het Hof van Cassatie van 28 maart 2017. Daarin geeft Hof van Cassatie een moderne interpretatie van artikel 26 Wpa en is het Hof van oordeel dat artikel 26 Wpa een rechtsgrond biedt voor het betreden van *online* publiek toegankelijke plaatsen door de politie.

De Agora-zaak

Het Hof van Cassatie geeft deels invulling aan het vraagstuk hoever de online bevoegdheden van de politie gaan. De politie had zich in deze zaak op het Agoraforum, een online zwarte markt waar onder meer drugs werden verhandeld, begeven zonder bijzondere machtiging daarvoor. Om toegang te krijgen werd anonimiserende software gebruikt (TOR-software), de politie kreeg daarnaast toegang tot het forum door een uitnodigingslink van een lid van het forum te ontvangen, en de onderzoekers maakten gebruik van een alias. Het Hof van Cassatie oordeelde dat er in dit geval sprake was van een voor het publiek toegankelijke plaats op het internet.¹¹⁵

Hierbij wordt opgemerkt dat het arrest is uitgesproken in de context van een strafzaak (behorend bij de gerechtelijke politie), waarbij het Wetboek van strafvordering de politiebevoegdheden regelt.

Todts¹¹⁶ is kritischer ten aanzien van de stelling dat artikel 26 Wpa ook geldt voor online onderzoek. Zij geeft aan dat artikel 26 Wpa niet geschreven is met het oog op (ook) online publiek toegankelijke plaatsen. Bovendien, zo geeft zij aan, moeten beperkingen op het fundamentele recht op privacy restrictief worden geïnterpreteerd, zodat de virtuele wereld niet zomaar onder deze bepaling kan worden begrepen. Als het gaat om online informatievergaring door *een bestuur*, bijvoorbeeld een gemeente, rijzen daarnaast vragen over de vereiste wettelijke grondslag.¹¹⁷

Ook Saelens¹¹⁸ wijst op de vraag in hoeverre bij online patrouilleren door de bestuurlijke politie persoonsgegevens kunnen worden verwerkt en of dat voorzienbaar is voor de burger in het licht van de EHRM-jurisprudentie die eist dat de wettelijke basis voldoende nauwkeurig en duidelijk moet zijn in het licht van de gestelde politiebevoegdheid.¹¹⁹ Volgens Saelens is het niet zonder meer duidelijk of, als de politie zich toegang verschaft tot de digitale wereld, onmiddellijk persoonsgegevens worden verwerkt, en zo ja, of de verwerking van persoonsgegevens noodzakelijk en proportioneel is. Als in de digitale omgeving (persoons)gegevens verwerkt worden is de grens tussen overmatige en proportionele gegevensverwerking soms flinterdun. Saelens wijst op artikel 44/1 Wpa op grond waarvan alleen persoonsgegevens verwerkt kunnen worden als daartoe grond bestaat en de verwerking van de persoonsgegevens noodzakelijk is. Daarvoor moet de bestuurlijke politie bij het online patrouilleren evenwel gedragingen of handelingen vaststellen die de openbare orde kunnen verstoren. Volgens Saelens is alleen de aanwezigheid van personen op online publiek toegankelijke plaatsen onvoldoende

¹¹⁴ J. C. CONINGS en P. VAN LINTHOUT, "Sociale media. Een nieuwe uitdaging voor politie en justitie", *Panopticon* 2012, afl. 3, 205-230.

¹¹⁵ Cass. 28 maart 2017, AR P.16.1245.N.

¹¹⁶ Liesbeth Todts is professor bestuursrecht bij Universiteit Gent, wetenschappelijk medewerker bij Universiteit Antwerpen en advocaat

¹¹⁷ L. Todts, De gemeentelijke bestuurlijke handhaving van ondermijnende criminaliteit: naar een (lokaal) bestuursstrafrecht? *Tijdschrift voor gemeenterecht*, 2024/3, p. 142-164.

¹¹⁸ Expert en commissaris-onderzoeker bij het COC en vrijwillig wetenschappelijk medewerker aan de Vrije Universiteit Brussel.

¹¹⁹ Saelens, Internetpatrouilleren in het kader van de bestuurlijke politie, p. 391-392.

om de verwerking te rechtvaardigen. De politieambtenaar kan dus niet zomaar persoonsgegevens verwerken, ook al heeft hij op grond van artikel 26 Wpa een grondslag voor toegang tot de online publiek toegankelijke plaats.¹²⁰

Gebruik van nepprofielen

In het arrest van het Hof van Cassatie werd geoordeeld dat het gebruik van een alias door de politie is toegestaan. Het Hof zegt hierover: *‘Het gebruik van een alias kan daarbij behoren tot de normale wijze van het bezoeken van delen van het internet, mits dat gebruik niet bestaat in het aannemen van een geloofwaardige fictieve identiteit en de gebruikte alias niet van aard is het plegen van een misdrijf uit te lokken.’*¹²¹ Met andere woorden: een politieagent mag zich online niet voordoen als een echt bestaande persoon, zoals Jan de Vries, maar wel als bijvoorbeeld Donald Duck, want dan is het voor iedereen duidelijk dat het geen echt persoon is.

Vragen aan de minister over mogelijkheden voor het gebruik van nep-profielen

In 2021 stelde een lid van de Senaat vragen aan de minister van Binnenlandse Zaken, Institutionele Hervormingen en Democratische Vernieuwing over het gebruik van nep-profielen door de Belgische politie. Aanleiding voor deze vragen was kritiek die in Nederland was ontstaan over het gebruik van nepaccounts door de politie.¹²²

Op de vraag of ordediensten gebruik maken van valse profielen antwoordt de minister als volgt: *‘In het raam van de monitoring van en het onderzoek op het internet maken de politiediensten geen gebruik van valse profielen, wel van «onderzoeksprofielen». Deze profielen moeten aan specifieke criteria voldoen om in overeenstemming te zijn met de wetgeving. Deze onderzoeksprofielen worden gebruikt bij de dagelijkse controle van open bronnen (bronnen die vrij toegankelijk zijn). Er dient evenwel een onderscheid te worden gemaakt tussen «monitoring van het internet» en «onderzoek op het internet». De monitoring of bewaking is de algemene en brede screening, met als doel fenomenen van bestuurlijke of van gerechtelijke aard die zich voordoen op het internet op te sporen. Onderzoek op het internet is het verzamelen van informatie, volgend op de vaststelling van een strafbaar feit tijdens de monitoring of bewaking. Monitoring van het internet moet worden gezien als een vorm van virtuele patrouille, met het in acht nemen van de bestaande wetgeving.’*¹²³

Vervolgens geeft de minister aan dat het wetgevend kader bestaat uit het eerder genoemde artikel 44/1 Wpa. De algemene omschrijving van dat artikel omvat volgens de minister ook de informatievergaring met behulp van open bronnen. Het gebruik van onderzoeksprofielen is volgens de minister een ‘uitoefening van een politiepatrouille in de virtuele wereld’ en zal, zolang het binnen de voorwaarden van rechtmatigheid en proportionaliteit blijft, van toepassing blijven.¹²⁴

5.3 De uitvoering van online informatievergaring

We hebben voor het eerste deelonderzoek twee interviews gehouden. Beide gesprekspartners geven aan dat de bestuurlijke politie in België gebruik maakt van online onderzoek voor

¹²⁰ Saelens, Internetpatrouilleren in het kader van de bestuurlijke politie, p. 392.

¹²¹ Cass. 28 maart 2017, AR P.16.1245.N, r.o. 3.

¹²² Daarbij werd verwezen naar dit artikel: <https://www.nrc.nl/nieuws/2021/05/27/kritiek-op-inzet-nepaccounts-door-politie-a4045203>

¹²³ [Schriftelijke vraag nr. 7-1261 \(senate.be\)](#)

¹²⁴ [Schriftelijke vraag nr. 7-1261 \(senate.be\)](#)

het handhaven van de openbare orde. Gesprekspartner geeft het voorbeeld dat social media in de gaten wordt gehouden of en waar er een illegale raveparty georganiseerd wordt.¹²⁵ Een andere reden waarom social media door de bestuurlijke politie in de gaten wordt gehouden is om bijvoorbeeld tijdig ongeplande betogingen te detecteren of om contact te leggen met de initiatiefnemer daarvan en om de dialoog aan te gaan.¹²⁶

Daarnaast geeft de voorzitter van het Controleorgaan op de Politie Informatie (COC) in een interview aan dat de werkwijze binnen de politiezones erg uiteenloopt en er weinig zicht is op wat de politie precies doet.¹²⁷

*'[...] de ene werkt al proactiever dan de andere of heeft veel meer financiële en digitale mogelijkheden dan de andere. Wat ze daar concreet allemaal doen en welke tools ze allemaal gebruiken in het kader van bestuurlijke politie, daar heeft niemand een globaal overzicht over.'*¹²⁸

Uit de literatuur volgt wel dat er in 2023 een ruime verspreiding was binnen de onderzochte politiezones¹²⁹ van niet-geautomatiseerd onderzoek in open bronnen. Deze brede verspreiding is volgens Van Biervliet en anderen mogelijk het resultaat van de toegankelijkheid van de technologie. Politieambtenaren kunnen namelijk op verschillende manieren open bronnen consulteren, bijvoorbeeld door personen op te zoeken op sociale media of door gebruik te maken van RSS-feeds. Geautomatiseerde vormen van dergelijk onderzoek, waaronder het gebruik van profiling software, zijn daarentegen minder breed verspreid binnen de onderzochte politiezones.¹³⁰ Ondanks dat politiezones bijvoorbeeld in het kader van evenementen of betogingen samenwerken komt uit de gevoerde interviews het beeld naar voren dat dit niet leidt tot kennisoverdracht op het gebied van onderzoek in open bronnen tussen de politiezones. Een reden daarvoor lijkt volgens een geïnterviewde te zijn gelegen in het feit dat het uitvoeren van dergelijk onderzoek niet ligt binnen de taken van de in het kader van de samenwerking uitgeleende politieambtenaren.

5.4 Toezicht

Het toezicht op de politie in België is verdeeld over verschillende instanties. Ten eerste kennen de lokale politiezones en de federale politie een Dienst Intern Toezicht (DIT). Deze dienst onderzoekt klachten of meldingen over het optreden van de korpsleden. De interne controlefunctie moet aan de ene kant bijdragen aan kwaliteitsverbetering op het gebied van bedrijfsprocessen en aan de andere kant bijdragen aan het functioneren van medewerkers. Ten tweede is er de Algemene Inspectie van de federale politie en van de lokale politie (AIG). Dit is een inspectie en auditdienst die de werking van de federale politie en de lokale politie controleert. De AIG werkt onafhankelijk van de politie. Ten derde bestaat het Comité P. Dit is een onafhankelijk toezichtsorgaan die onder meer toezicht houdt op de bescherming van de rechten van burgers. Met betrekking tot het verwerken van persoonsgegevens is met name het

¹²⁵ Zie ook vrt.be, 4 augustus 2023, <https://www.vrt.be/vrtnws/nl/2023/08/04/kanne-in-riemst-door-politie-hermetisch-afgesloten-om-illegale-r/>.

¹²⁶ Zie ook ministerie van Binnenlandse Zaken, ministeriële omzendbrief OOP 41bis betreffende de operationalisering van het referentiekader CP 4bis over het genegotieerd beheer van de openbare ruimte van 30 januari 2025, par. 4.1.

¹²⁷ Zie ook Lodewijk Gunther Moor, Toezicht op de politie, 2020-2, nr. 55, p.146.

¹²⁸ <https://www.knack.be/nieuws/belgie/online-patrouilleren-wat-de-politie-wel-en-niet-mag/>

¹²⁹ In het onderzoek zijn de politiezones in Vlaanderen en het Brussels Hoofdstedelijk Gewest bevestigd. In totaal reageerden 86 van de 113 korpschefs in Vlaanderen en het Brussels Hoofdstedelijk Gewest. Donatella Van Biervliet, Jeroen Maesschalck, Lore Rooseleers (2024), Technologie in de Belgische lokale politie: Een bredere verspreiding?, Panopticon 45(5), par. 2.1

¹³⁰ Zie Donatella Van Biervliet, Jeroen Maesschalck, Lore Rooseleers (2024), Technologie in de Belgische lokale politie: Een bredere verspreiding?, Panopticon 45(5), p. 421-442.

Controleorgaan op de Politie Informatie (COC) een relevante autoriteit. Het COC is in België de gegevensbeschermingsautoriteit voor onder meer de federale en lokale politie. Het idee achter een aparte gegevensbeschermingsautoriteit voor de politie is dat de juridische context van de gegevensverwerking op veel punten afwijkt, net als de praktische situatie omtrent de verzameling en verwerking van deze gegevens. Door een gespecialiseerde toezichthouder op te zetten zou het toezicht effectiever kunnen worden ingericht.¹³¹ Het COC heeft tot op heden geen onderzoek verricht naar het gebruik van online gegevensverwerking bij de bestuurlijke politie ter handhaving van de openbare orde.

5.5 Inzet van technische hulpmiddelen

Bewakingscamera's en ANPR-systemen

Bewakingscamera's hebben tot doel de bewaking en het toezicht van plaatsen en verwerken daarvoor beelden.¹³² Regels voor de inzet en het gebruik van bewakingscamera's zijn vastgelegd in verschillende regelingen. Zo is er onder meer wetgeving in het gebruik van bijzondere opsporingsmethodes,¹³³ voor bewakingscamera's in het algemeen¹³⁴ en voor bewakingscamera's in voetbalstadions.¹³⁵

Het gebruik van camera's door de politie wordt sinds de inwerkingtreding van de AVG in 2018 niet meer geregeld door de Camerawet, maar door de WPA. Camera's van andere partijen zoals steden en gemeenten, worden nog wel geregeld door de Camerawet.¹³⁶ Daarnaast zijn in principe ook de AVG en de Belgische uitvoeringswet van de AVG van toepassing. Als de gegevensverwerking gebeurt door politiediensten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, dan is niet de AVG maar enkel titel 2 van de Belgische uitvoeringswet, waarin Richtlijn gegevensbescherming bij rechtshandhaving (Richtlijn (EU) 2016/680) in is geïmplementeerd, van toepassing.^{137,138}

Cameragebruik door de politie

De plaatsing van camera's door een politiedienst wordt beheerd door de principes van proportionaliteit, subsidiariteit, finaliteit en doelmatigheid. Bij de inzet van camera's door de politie kan onderscheid worden gemaakt tussen zichtbaar en niet-zichtbaar gebruik van camera's. Het zichtbaar gebruik van camera's voor het inwinnen van informatie door de bestuurlijke politie is alleen toegestaan in de volgende gevallen (artikel 25/3 §2 jo. 44/5 § 1, 2° tot 5°):

1. de contactgegevens van de vertegenwoordigers van verenigingen die vrijwillig door laatstgenoemden worden meegedeeld of die openbaar beschikbaar zijn, om het beheer van gebeurtenissen mogelijk te maken;

¹³¹ [3031-de-verwerking-van-politiegegevens-in-vijf-Europese-landen-volledige-tekst.pdf \(wodc.nl\)](#)

^{132,133} Art. 2 onder 4 Camerawet.

¹³³ Wet 6 januari 2003 op de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden (BOM-wet).

¹³⁴ Camerawet

¹³⁵ KB 12 september 1999 betreffende de installatie en de werking van bewakingscamera's in de voetbalstadions.

¹³⁶ F. Schram, de camerawetgeving en haar actuele betekenis voor de lokale en federale politie, in *De sluier rond anonimiteit opgelicht...*, p. 254.

¹³⁷ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

¹³⁸ F. Schram, de camerawetgeving en haar actuele betekenis voor de lokale en federale politie, in *De sluier rond anonimiteit opgelicht...*, p. 256.

2. de gegevens met betrekking tot de personen die betrokken zijn bij fenomenen van bestuurlijke politie waaronder verstaan wordt het geheel van problemen die de openbare orde verstoren en die gepaste maatregelen van bestuurlijke politie vereisen omdat zij van dezelfde aard en terugkerend zijn, door dezelfde personen gepleegd worden of gericht zijn op dezelfde categorieën van slachtoffers of plaatsen;
3. de gegevens met betrekking tot de leden van een nationale of internationale groepering die de openbare orde zoals bedoeld in artikel 14 zou kunnen verstoren;
4. de gegevens met betrekking tot de personen die schade kunnen toebrengen aan te beschermen personen of roerende en onroerende goederen en de gegevens met betrekking tot de personen die er het doelwit van kunnen uitmaken;
5. de gegevens met betrekking tot de in de artikelen 18 tot 21 bedoelde personen;¹³⁹ de gegevens met betrekking tot de personen die geregistreerd zijn inzake gerechtelijke politie voor een strafbaar feit dat gepleegd werd in het kader van de openbare orde-handhaving;

Automatic Number Plate Recognition (ANPR) is een vorm van technologisch toezicht waarbij camera's automatisch kentekens herkennen. Na de aanslagen in Parijs vaardigde de regering eind 2015 in de strijd tegen terrorisme een aantal maatregelen uit, waarvan de uitbreiding van het netwerk van ANPR-camera's één van de speerpunten was.¹⁴⁰ Er zou één nationale bank-office (ANPR Managed Services (AMS)) worden geïmplementeerd waarop alle ANPR-camera's zouden worden aangesloten. Dit laatste is nog niet gebeurd, waardoor sommige camera's aangesloten zijn op het landelijke AMS-systeem, maar andere camera's zijn aangesloten op de lokale gegevensbank van de lokale politie of stad of gemeente.¹⁴¹

In 2023 heeft de federale regering beslist dat de federale politie het netwerk van ANPR-camera's op termijn tot 10.000 camera's kan uitbreiden. De ANPR-camera's worden ingezet voor steeds meer uiteenlopende doelen, zoals het betrappen van een telefonerende autobestuurder of het controleren van de avondklok tijdens de coronacrisis.¹⁴² De Korpschef van een Vlaamse politiezone omschreef de mogelijkheden van installatie van nieuwe ANPR-camera's als volgt:

*"Met de installatie en activatie van ons ANPR-systeem verbetert de politiezone het aan haar grenzen. Het zal ons helpen bij het efficiënter uitvoeren van onze opdrachten van bestuurlijke en gerechtelijke politie. Dit zowel op vlak van verkeersveiligheid (ontdekken van onder andere niet-verzekering voertuigen, verkeersrecidivisten, rijverboden) als bij de opsporing van daders van criminaliteit en overlast bv. bij inbraken in gebouwen, het onderzoeken van verdachte situaties of verdacht gemelde gedragingen. Het systeem geeft ons ook de mogelijkheid om meer doelgericht te gaan werken."*¹⁴³

Eerder waarschuwde Vast Comité van Toezicht op de Politie op basis van data uit 2020 voor een soms beperkte betrouwbaarheid van de hits en een versnipperde operationele respons bij gestolen nummerplaten, met mogelijk gevaarlijke situaties voor politieambtenaren tot

¹³⁹ Het gaat daarbij om toezicht op geesteszieken (art. 18), geïnterneerden (art. 19) en veroordeelden in vrijheid (art. 20).

¹⁴⁰¹⁴⁰ Zie ook [rapport van het onderzoek naar het functioneren van de geïntegreerde politie inzake ANPR-hit-afhandeling van gestolen nummerplaten.pdf](#).

¹⁴¹ Kenniscentrum Data & Maatschappij, Rapport over bevoegdheden in het delen van gegevens, Automatische kentekenplaat-herkenning als toepassingsgeval, 2021, p. 22-23.

¹⁴²¹⁴² [Steeds meer camera's in het straatbeeld: "Ze voorkomen criminaliteit niet, de samenleving wordt er niet beter van" | VRT NWS: nieuws](#)

¹⁴³ <https://www.politie.be/5437/nieuws/nieuwe-anpr-cameras-versterken-veiligheid>.

gevolg. Een hoog percentage van zogenoemde foute reads zou er namelijk voor kunnen zorgen dat politieambtenaren onnodige risico's moeten nemen.¹⁴⁴

Naar aanleiding van het invoeren van specifieke regels voor politiediensten met betrekking tot camera's in de WPA, heeft de wetgever ook een nieuw soort politionele gegevensbanken ingevoerd, namelijk de technische gegevensbanken. Op die manier konden afwijkende regels worden vastgesteld die meer garanties zouden bieden dan de voor andere databanken bestaande regels. De WPA kent op dit moment alleen een technische gegevensbank als gevolg van het gebruik van enerzijds intelligente camera's en anderzijds intelligente systemen voor ANPR.¹⁴⁵

Een technische gegevensbank is een verzamelplaats voor persoonsgegevens van technische aard, afkomstig uit technische tools. De WPA regelt dat de gegevens uit de lokale technische ANPR-gegevensbanken van de politie moeten worden doorgezonden naar de landelijke gegevensbank.¹⁴⁶ Van daaruit zijn ze onder voorwaarden in raadpleegbaar voor alle politiediensten in het land.¹⁴⁷ Lokale overheden kunnen op dit moment alleen toegang krijgen tot ANPR-gegevens in het AMS-systeem, als dit nodig is in het kader van wettelijke opdrachten en op voorwaarde dat er een link is met de openbare veiligheid (bijvoorbeeld rampenbestrijding).¹⁴⁸

In de technische gegevensbank worden de volgende gegevens vastgelegd:¹⁴⁹

1. de datum, het tijdstip en de precieze plaats van langsrijden van de nummerplaat,
2. de kenmerken van het voertuig dat verbonden is aan deze nummerplaat,
3. een foto van de nummerplaat aan de voorkant van het voertuig en in voorkomend geval, aan de achterkant,
4. een foto van het voertuig,
5. in voorkomend geval, een foto van de bestuurder en van de passagiers,
6. de logginggegevens van de verwerkingen.

De doeleinden voor het oprichten en gebruiken van de technische gegevensbanken zijn beperkt en worden uitdrukkelijk door de wet bepaald, zowel voor de bestuurlijke als de gerechtelijke politie. Voor de bestuurlijke politie geldt dat het gebruik en oprichten van de gegevensbank mag in het kader van de hulp bij uitvoering van de opdrachten van bestuurlijke politie voor de categorieën personen bedoeld in artikel 44/5 § 1, 2° tot 5° (zie de eerdere opsomming).

¹⁴⁴ Vast Comité van Toezicht op de politiediensten. (2022). Het functioneren van de geïntegreerde politie inzake ANPR-hit afhandeling van gestolen nummerplaten, hoofdstuk 5. Zie ook Donatella Van Biervliet, Jeroen Maesschalck, Lore Rooseleers (2024), Technologie in de Belgische lokale politie: Een bredere verspreiding?, Panopticon 45(5), par. 3.1

¹⁴⁵ Art. 44/2 3: "Wanneer in de uitvoering van de opdrachten van bestuurlijke en gerechtelijke politie, technische hulpmiddelen worden gebruikt om automatisch persoonsgegevens en informatie van technische aard te verzamelen, zodanig gestructureerd dat zij rechtstreeks kunnen worden teruggevonden, worden deze gegevens verwerkt in een technische gegevensbank. Een technische gegevensbank wordt gecreëerd ingevolge het gebruik van:

1° intelligente camera's voor de automatische nummerplaatherkenning;

2° intelligente systemen voor de automatische nummerplaatherkenning.

Onder intelligente systemen voor de automatische nummerplaatherkenning wordt verstaan elke intelligente software die het mogelijk maakt om automatisch de door camera's

¹⁴⁶ Art. 44/11/3sexies.

¹⁴⁷ Art. 44/11/3sexies §2 WPA; Kenniscentrum Data & Maatschappij, Rapport over bevoegdheden in het delen van gegevens, Automatische kentekenplaatherkenning als toepassingsgeval, 2021, p. 22.

¹⁴⁸ Art. 44/11/7 WPA: "De persoonsgegevens en informatie worden meegedeeld aan de bevoegde gerechtelijke overheden of overheden van bestuurlijke politie om hen toe te laten hun wettelijke opdrachten uit te oefenen" en art. 14 WPA ("Bij het vervullen van hun opdrachten van bestuurlijke politie, zien (de politiediensten) toe op de handhaving van de openbare orde met inbegrip van de naleving van de politiewetten en -verordeningen, de voorkoming van misdrijven en de bescherming van personen en goederen").

¹⁴⁹ Art. 44/11/3decies WPA.

De WPA bepaalt op strikte wijze op welke manier, voor hoelang en met welke toestemming de bestuurlijke of gerechtelijke politie kan overgaan tot bijvoorbeeld gerichte opsporingen of tot correlaties. De WPA bevat garanties om te verzekeren dat gegevens alleen in een strikt omljnd kader geraadpleegd en gebruikt kunnen worden.¹⁵⁰

Cameragebruik door gemeenten

Voorwaarden voor de inzet van camera's door gemeenten volgen uit de Camerawet, de AVG en de Belgische uitvoeringswet. In de Camerawet wordt onderscheid gemaakt tussen (tijdelijk) vaste en mobiele bewakingscamera's.

Plaatsing en gebruik van (tijdelijk) vaste bewakingscamera's

Het plaatsen van camera's in niet-besloten plaatsen kan slechts worden gedaan door een openbare overheid, zoals een gemeente.¹⁵¹ Het plaatsen van deze camera's kan pas na het verkrijgen van een positief advies van de gemeenteraad. De gemeenteraad verstrekt advies na de korpschef van de politiezone te hebben geraadpleegd.¹⁵²

Het bekijken van de camerabeelden in *real time* is uitsluitend toegestaan onder toezicht van de politiediensten, zodat deze diensten onmiddellijk kunnen ingrijpen bij bijvoorbeeld overlast of verstoring van de openbare orde en deze diensten in hun optreden optimaal kunnen worden gestuurd.¹⁵³ De toegang tot deze beelden in real time is ook toegestaan om het de bevoegde overheden en diensten mogelijk te maken om de veiligheid bij belangrijke evenementen die een impact kunnen hebben op de openbare orde en veiligheid van de bevolking te coördineren.¹⁵⁴ Het opnemen van deze beelden mag alleen om bewijzen te verzamelen van overlast of om bijvoorbeeld verstoorders van de openbare orde op te sporen en te identificeren. Als deze beelden geen bijdrage kunnen leveren aan het bewijzen daarvan, worden de beelden in principe niet langer dan één maand bewaard.¹⁵⁵

Gebruik van mobiele bewakingscamera's

Mobiele bewakingscamera's mogen in niet-besloten plaatsen alleen gebruikt worden met het oog op de automatische nummerplaatherkenning, door of in opdracht van de gemeentelijke overheden worden gebruikt voor het voorkomen, vaststellen of opsporen van overlast in de zin van artikel 135 van de nieuwe gemeentewet.¹⁵⁶ Ook voorafgaand aan de beslissing om gebruik te maken van mobiele camera's moet eerst positief advies van de gemeenteraad verkregen zijn. De gemeenteraad verstrekt het advies na het raadplegen van de korpschef en bepaalt de geldigheidsduur van het advies.¹⁵⁷

¹⁵⁰ F. Schram, de camerawetgeving en haar actuele betekenis voor de lokale en federale politie, in *De sluier rond anonimiteit opgelicht...*, p. 254.

¹⁵¹ Art. 5 §1 Camerawet

¹⁵² Art. 5 §2 Camerawet

¹⁵³ Art. 5 §4 Camerawet

¹⁵⁴ Art. 5 §4 Camerawet

¹⁵⁵ Art. 5 §4 Camerawet

¹⁵⁶ Art. 7/1 Camerawet

¹⁵⁷ Art. 7/1 Camerawet

6. Ierland

6.1 Organisatie van de openbare ordehandhaving

In Ierland is de Garda Síochána (Hierna: de Garda) verantwoordelijk voor alle soorten politietaken, van patrouilleren en opsporing tot forensisch onderzoek en verkeershandhaving en handhaving van de openbare orde. De Garda is een gecentraliseerde organisatie onder leiding van de Garda Commissioner, die wordt benoemd door de Ierse regering. Het land is verdeeld in regio's, elk met een regionaal hoofdkwartier. Elke regio is onderverdeeld in divisies, elk met een divisiehoofdkwartier. De divisies zijn onderverdeeld in subdistricten, elk met een politiebureau.

Naast de reguliere politiedienst heeft de Garda ok gespecialiseerde eenheden, zoals de Criminal Investigation Division (CID), Drugs and Organised Crime Bureau (DOCB), de Armed Support Units (ASU) – om te reageren op specifieke uitdagingen zoals georganiseerde misdaad en terrorisme – en de Public Order Units. Deze laatstgenoemde eenheden zijn belast met het handhaven van de openbare orde en veiligheid.

6.2 Het wettelijk kader voor de uitoefening van de openbare ordetaak

Openbare ordewetgeving

In Ierland vindt de openbare ordehandhaving plaats binnen het kader van verschillende wetten en regelgeving. Het gaat daarbij om de Garda Síochána Act 2005. Deze wet bepaalt de bevoegdheden en taken van de Garda. De wet geeft de Garda de algemene bevoegdheid om toezicht te houden op openbare plaatsen ter voorkoming van misdaad en ter bescherming van de openbare veiligheid. De Public Order Act 1994 en de Criminal Justice Act voorzien in de handhaving van de openbare orde en de bestrijding van verstoring en wanordelijken, door bepaalde gedragingen strafbaar te stellen. De Criminal Law (Riots) Act 1994 voorziet in de aanpak van rellen en gerelateerde misdrijven, en geeft de autoriteiten de bevoegdheid om op te treden.

De Criminal Justice (Surveillance) Act 2009 regelt het gebruik van heimelijk toezicht door de Garda. De wet bepaalt dat de Garda alleen heimelijk toezicht mag gebruiken als dat noodzakelijk is voor het voorkomen of opsporen van een ernstig misdrijf.

Bevoegdheden om online informatie te vergaren met het oog op openbare ordehandhaving

In Ierland zijn er geen specifieke wetten die exclusief zijn gewijd aan online monitoring door de Garda. Wel heeft de Garda een beleidsdocument opgesteld gericht op Open Source Intelligence. Dit beleidsdocument bevat algemeen geformuleerde uitgangspunten.

Uit dit beleidsdocument kan worden afgeleid dat de Garda toegang heeft tot openbaar beschikbare informatie op sociale mediaplatforms, zoals openbare berichten, profielen of pagina's, en dit kan worden beschouwd als legitiem gebruik van informatie. Wel dient de Garda bij het doen van dergelijk onderzoek de Code of Ethics for the Garda Síochána, An Garda Síochána Code, Chapter 6, Employment, Equality and Ethics, The Garda Síochána Act, 2005, Data Protection Act, 2018, An Garda Síochána Data Protection Code of Practice, ICT Acceptable Usage Policy, Mobile Device Procedure, Code of Practice – CHIS, 10. HQ Directive 19/19 Human Rights Framework in aanmerking te nemen.¹⁵⁸

In de praktijk zal het doen van online onderzoek ook moeten voldoen aan het beleidsdocument 'Garda Decision Making Model'.¹⁵⁹ Dit document helpt de Garda om tot een afgewogen beslissingen te komen bij de uitvoering van de politietaak, waarbij het waarborgen van grond- en mensenrechten voorop staat. Het doen van onderzoek en daaronder begrepen online onderzoek is een onderdeel van dit beslismodel. Aan de hand van vragen wordt de Garda geholpen om onderzoek te doen dat proportioneel en noodzakelijk is.

De Telecommunications (Retention of Data) Act regelt het bewaren van telecommunicatiegegevens, inclusief internetgegevens, voor wetshandavingsdoeleinden. Het Hof van Justitie van de Europese Unie heeft bepaald dat de verplichte bewaring zonder enige voorafgaande controle ongrondwettig is. In 2023 is om die reden de wet aangepast. Wetshandavingsinstanties, zoals de politie, hebben het recht om toegang te krijgen tot deze bewaarde gegevens onder bepaalde voorwaarden en met de juiste wettelijke procedures. Dit kan onder meer vereisen dat de politie een gerechtelijk bevel of een soortgelijke juridische autorisatie krijgt voordat ze toegang krijgen tot de gegevens.

Privacywaarborgen

Alle wetten benoemd in paragraaf 1.2.1 bevatten waarborgen om de inzet van monitoring in balans te brengen met de privacy en daarmee in overeenstemming te handelen met de EU-richtlijn 2016/680.

De Garda Síochána Act 2005 bepaalt dat de Garda haar politietaken alleen mag uitvoeren voor een van de in de wet genoemde doeleinden, zoals het voorkomen of opsporen van een misdrijf, het beschermen van de nationale veiligheid of het handhaven van de openbare orde.¹⁶⁰ De Garda Síochána Act 2005 verplicht de Garda Commissioner om een Code of Ethics op te stellen omtrent het handelen van de politie.¹⁶¹ Deze code benadrukt het belang van het respecteren van grondrechten en menselijke waardigheid. Er is een onderdeel gewijd aan informatie en privacy die onder andere, benadrukt dat een inbreuk op het recht op privacy alleen is toegestaan in het geval deze inbreuk noodzakelijk is om een legitiem doel te dienen, en dat informatie wordt verzameld in overeenstemming met de regels omtrent gegevensbescherming.

¹⁵⁸ Open Source Intelligence, Garda Síochána, 10 januari 2023, p. 2

¹⁵⁹ Garda Decision Making Model, Garda Síochána, 5 december 2022, p. 4-7.

¹⁶⁰ Sectie 7 Garda Síochána Act 2005

¹⁶¹ Sectie 17 Garda Síochána Act 2005.

De Criminal Justice (Surveillance) Act 2009 bevat waarborgen om de privacy van betrokkene te beschermen, door randvoorwaarden te stellen aan het gebruik van covert surveillance. De wet legt vast dat het uitvoeren van surveillanceactiviteiten alleen kan plaatsvinden met de juiste juridische autorisatie.¹⁶² Daarnaast bepaalt de wet dat surveillanceactiviteiten alleen kunnen worden uitgevoerd voor specifieke wettelijke doeleinden, zoals het voorkomen of onderzoeken van ernstige misdrijven, waaronder terrorisme, georganiseerde misdaad en drugs-handel. Deze wet ziet niet op de handhaving van de openbare orde door de Garda.

De Garda valt onder het toezicht van Data Privacy Commissioner (DPC), die als onafhankelijk toezichthouder is aangewezen als bedoeld in de Algemene verordening gegevensbescherming en de EU-richtlijn 2016/680.

6.3 De uitvoering van online informatievergaring

Binnen de Garda zijn verschillende afdelingen en eenheden die zich bezighouden met het monitoren van online activiteiten en het verzamelen van informatie uit digitale bronnen, waaronder Public Order Units. Deze eenheden kunnen online dreigingen die kunnen leiden tot verstoringen van de openbare orde monitoren.

Onderkend wordt dat het monitoren van online activiteiten en het uitvoeren van online onderzoeken vaak gespecialiseerde vaardigheden vereisen. De medewerkers van de Garda die OSINT gebruiken en online onderzoeken uitvoeren, hebben een belangrijke informatiepositie die bijdraagt aan alle aspecten van het politiewerk en waardevolle informatie levert ter ondersteuning van andere op inlichtingen gebaseerde resultaten.¹⁶³ De Garda heeft extra middelen gekregen om online informatie te vergaren om de openbare orde te handhaven en de Garda werkt aan het verbeteren van het gebruik van sociale media en open source voor politiedoeleinden.¹⁶⁴ Ook vanuit de Oireachtas, het Iers parlement, is er aandacht voor de rol van het doen van online onderzoek in het kader van de handhaving van de openbare orde naar aanleiding van enkele incidenten, onder meer in Dublin.¹⁶⁵

Daarnaast zoekt de Garda actieve samenwerking met andere organisaties, waaronder sociale mediabedrijven om desinformatie en geruchten die op de verschillende platformen circuleren tegen te gaan, vooral wanneer incidenten plaatsvinden die van invloed zijn op de openbare orde.

6.4 Inzet van technische hulpmiddelen

Cameratoezicht

In Ierland worden technische hulpmiddelen ingezet bij het handhaven van de openbare orde. Zo wordt er veelvuldig gebruik gemaakt van cameratoezicht. Garda heeft een uitgebreid netwerk van camera's in steden en dorpen in heel Ierland. Sectie 38 van de Garda Síochána Act bepaalt dat de Garda Commissioner de installatie en operationalisering van een CCTV met het doel om de openbare orde te handhaven in de openbare ruimte. De Garda Commissioner

¹⁶² Sectie 3 Criminal Justice (Surveillance) Act 2009.

¹⁶³ Open Source Intelligence, Garda Síochána, 10 januari 2023, p. 2

¹⁶⁴ The future of policing in Ireland, Garda Síochána, September 2018

¹⁶⁵ Connect: An Garda Síochána Digital Strategy 2019 – 2023. Garda Síochána, not dated.

¹⁶⁶ Zie onder meer Committee of public accounts debate: Vote 20 – An Garda Síochána, Iers Parlement, 21 maart 2024.

moet de gebieden specificeren waar, op basis van de beschikbare informatie, de installatie en het gebruik van CCTV gerechtvaardigd is voor het in Sectie 38 vermelde doel. Daarnaast zijn specifieke richtlijnen opgesteld die bepalingen bevat over plaatsing, opslag, toegang en rechten van individuen.

Automatische nummerplaatherkenning (ANPR)

Garda gebruikt ANPR systemen om gestolen voertuigen te identificeren, voertuigen te controleren die aan misdaad zijn gekoppeld en voor het overtreden van verkeersovertredingen, worden ANPR-systemen ingezet van het monitoren van grote evenementen. De Ierse politie heeft een richtlijn opgesteld voor het gebruik van ANPR-systemen.

Lichaamscamera's

Garda gebruikt lichaamscamera's voor het vastleggen van de interactie met het publiek, het verzamelen van bewijsmateriaal voor misdrijven en overtredingen en het beschermen van politieagenten. Voor het gebruik van deze lichaamscamera's heeft de Ierse politie een richtlijn opgesteld.

Drones

Voor de handhaving van de openbare orde kan de Garda ook drones inzetten, zoals voor het monitoren van grote evenementen en het handhaven van verkeersregels. Voor het gebruik van deze drones heeft de Ierse politie een richtlijn opgesteld.

6.4.1 Toezicht op het gebruik van technische hulpmiddelen

De Garda heeft een eigen Directorate of Internal Affairs die verantwoordelijk is voor het onderzoeken van klachten over het wangedrag van politieagenten, inclusief het oneigenlijk gebruik van technische middelen. Daarnaast is er een code of Ethics die richtlijnen bevat over het gebruik van technische hulpmiddelen door de politie.

Garda is verplicht om jaarlijks verslag uit te brengen over het gebruik van technische middelen. De Data Protection Commissioner is een onafhankelijke instantie die toezicht houdt op het gebruik van persoonsgegevens door de Garda, inclusief het gebruik van technische middelen die persoonsgegevens verzamelen.

De Garda Síochána Ombudsman Commission is een onafhankelijke instantie die klachten over de Garda onderzoekt, inclusief klachten over het gebruik van technische middelen.

In bepaalde gevallen kan het gebruik van technische hulpmiddelen door de politie onderhevig zijn aan rechterlijke toetsing, zoals het verkrijgen van gerechtelijke bevelen voor het uitvoeren van surveillanceactiviteiten of het verkrijgen van toestemming van een rechter voor het uitvoeren van bepaalde ingrijpende maatregelen.

7. Denemarken

7.1 Organisatie van de openbare ordehandhaving

In Denemarken is de Deense politie verantwoordelijk voor het handhaven van de openbare orde, waarbij hun doelstelling en taken zijn vastgelegd in de *Bekendtgørelse af lov om politiets virksomhed*" (Politiewet). Deze wet biedt het juridische kader voor de werking van de politie, hun verantwoordelijkheden, en hoe zij hun taken uitvoeren met betrekking tot handhaving van de wet. De specifieke taken van de Deense politie omvatten het voorkomen van strafbare feiten, het verstoren van de openbare vrede en orde, het beschermen van individuen en de publieke veiligheid, het beëindigen van criminele activiteiten en het onderzoeken en vervolgen van strafbare feiten.

De Deense politie is verdeeld in 14¹⁶⁷ politiedistricten, elk geleid door een commissaris. Als hoofd van het politiedistrict draagt de commissaris de verantwoordelijkheid voor de dagelijkse leiding en de gevolgen van de politiewerkzaamheden binnen het desbetreffende geografische gebied, waaronder openbare orde handhaving.

De commissarissen van de 14 politiedistricten vormen samen een verenigd managementteam, aangevoerd door de Nationale Politiecommissaris. De Nationale Commissaris is verantwoordelijk voor de algemene leiding en draagt zorg voor de professionele, financiële en administratieve aspecten van de Deense politie. Hij of zij rapporteert direct aan de Minister van Justitie.

De politie kan bij de handhaving van de openbare orde worden ondersteund door de gemeentelijke handhavingsdienst (Kommunal forvaltning), de Home Guard (Hjemmeværnet) en het Deense leger (Forsvaret). Denk hierbij met name aan ondersteuning bij grotere evenementen om de veiligheid en orde te handhaven, bijvoorbeeld door het beheersen van menigten.

¹⁶⁷ De politiemacht van Denemarken, inclusief de gebieden van de Faeröer en Groenland, fungeert als een enkele nationale entiteit. Hoewel Groenland en de Faeröer buiten het Europese deel van Denemarken liggen, maken zij als onafhankelijke politiedistricten deel uit van het Koninkrijk Denemarken. Daarmee telt de Deense politie in totaal 14 districten, waarvan er twee zich buiten Europa bevinden.

7.2 Het wettelijk kader voor de uitoefening van de openbare ordetaak

Openbare ordewetgeving

Het belangrijkste kader wat betreft openbare ordehandhaving is de Politiewet. In paragrafen 3-6a zijn de bevoegdheden en maatregelen van de politie voor het handhaven van de openbare orde uiteengezet. De politie heeft onder meer de bevoegdheid om gebieden te ontruimen, af te zetten en de identiteit van personen te controleren of personen te fouilleren indien nodig om ordeverstoringen te voorkomen. Paragrafen 7-9 gaan over de bevoegdheden van de politie bij openbare bijeenkomsten, waarbij de politie de plicht heeft om de bijeenkomsten te begeleiden met het oog op een veilig verloop van deze bijeenkomsten. Ook worden de omstandigheden geschetst waarin de politie kan ingrijpen bij openbare bijeenkomsten die de openbare orde verstoren. Dit omvat het uitvaardigen van bevelen om een bijeenkomst te verplaatsen, voorwaarden te stellen ten aanzien van de uitvoering ervan, of bijeenkomsten ronduit te verbieden als deze worden beschouwd als een bedreiging voor de openbare vrede.

De Bekendtgørelse om politiets sikring af den offentlige orden og beskyttelse af enkeltpersoners og den offentlige sikkerhed mv., samt politiets adgang til at iværksætte midlertidige foranstaltninger (de Wet Openbare Orde) richt zich op het handhaven van de openbare orde en het beschermen van individuele en publieke veiligheid in Denemarken. Hoofdstuk 2 van de Openbare Orde Wet bevat regels tegen het veroorzaken van overlast op openbare plaatsen. Hoofdstuk 3 van de wet beschrijft de bevoegdheden van de politie om tijdelijke maatregelen te nemen in de vorm van bevelen of verboden om potentiële risico's voor de openbare orde of veiligheid te voorkomen. De politie kan activiteiten verbieden of beperkingen opleggen als dit wordt gezien als noodzakelijk om de openbare orde te kunnen handhaven. Deze maatregelen moeten worden genomen door de politiechef of iemand die daartoe door hem gemandateerd is. Daarnaast moeten de besluiten openbaar worden gemaakt met een verklaring van de redenen, locatie, en de duur van de maatregel. Er worden in de wet specifieke beperkingen of vereisten genoemd die de politie kan opleggen, waarbij kan worden gedacht aan het opleggen van gebieds- of samscholingsverboden.

Verder zijn er meerdere wettelijke regelingen die zien op de handhaving van de openbare orde in specifieke situaties, zoals regels over de handhaving van de openbare orde bij sportieve evenementen. Regels hieromtrent zijn neergelegd in de *Bekendtgørelse af lov om sikkerhed ved bestemte idrætsbegivenheder* (Wet openbare orde bij sportevenementen). De wet biedt de politie onder meer de mogelijkheid voor de politie om een gebiedsverbod op te leggen aan personen die verdacht worden van het verstoren van de openbare orde tijdens sportevenementen.

Bevoegdheden om online informatie te vergaren met het oog op openbare ordehandhaving

Het belangrijkste kader is de Politiewet. Paragraaf 2a, lid 2 van deze wet geeft de Deense politie de bevoegdheid om informatie uit openbaar toegankelijke bronnen te verzamelen en te verwerken wanneer dit nodig is voor de uitvoering van hun taken. Zoals al eerder is benoemd is het een taak van de Deense politie is om verstoringen van de openbare orde te voorkomen. De politie mag dus informatie verzamelen uit openbaar toegankelijke (online) bronnen, inclusief sociale media en andere platforms, om inzicht te krijgen in geplande evenementen of mogelijke bedreigingen. Hiervoor is vooraf geen specifieke toestemming nodig.

Paragraaf 2 van de Politiewet stelt dat de Minister van Justitie nader regels vaststelt over hoe de politie met (online) informatie omgaat. Door nadere regels te stellen kunnen doeleinden waarvoor online informatie kan worden verwerkt worden afgebakend. Echter lijkt er tot op heden geen nadere regels te zijn opgesteld over het doen van online onderzoek.

Privacywaarborgen

Hoewel de politie de bevoegdheid heeft om openbaar toegankelijke informatie te verzamelen, zijn er grenzen en toezichtsmechanismen om misbruik te voorkomen en de privacy van burgers te beschermen. Deel 3 van de *Lov om behandling af personoplysninger (Databeskyttelsesloven)*, waarin EU-richtlijn 2016/680 is geïmplementeerd, benadrukt de noodzaak van proportionaliteit en noodzakelijkheid bij het verzamelen en verwerken van persoonsgegevens door de politie, dus ook voor online gegevensverzameling. Gegevens mogen alleen worden verzameld voor een duidelijk doel dat past binnen de wettelijke taken van de politie. Er geldt een verbod op een verdere verwerking van gegevens voor andere doeleinden dan waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, tenzij dit is toegestaan bij wet en noodzakelijk en evenredig is met dat andere doel. Daarnaast is de politie verplicht te zorgen voor een goede beveiliging van de gegevens, mag informatie niet langer worden bewaard dan noodzakelijk is en personen wiens gegevens worden verwerkt hebben het recht op informatie, toegang, rectificatie en verwijdering van hun gegevens.

De *Datatilsynet* is Deense autoriteit voor gegevensbescherming is de onafhankelijke en externe autoriteit die toezicht houdt op de naleving van de regels voor de bescherming van persoonsgegevens in Denemarken. De bevoegdheden en taken zijn neergelegd in § 40, 41, 42 en 43 van de *Lov om behandling af personoplysninger (Databeskyttelsesloven)*. Wanneer de Deense gegevensbeschermingsautoriteit van mening is dat de politie de persoonsgegevens onterecht of onjuist verwerkt, kan zij een onderzoek instellen, corrigerende maatregelen treffen en gevraagd en ongevraagd advies geven. Ook heeft de Deense gegevensbeschermingsautoriteit de taak om het parlement te adviseren, de kennis van bewerkers te bevorderen en ziet zij toe de klachtenafhandeling

7.3 De uitvoering van online informatievergaring

De Deense politie heeft sinds 2022 een online patrouille eenheid.¹⁶⁸ Met dit initiatief vergroot de politie haar aanwezigheid in de digitale ruimte, vergelijkbaar met hun fysieke aanwezigheid in openbare ruimtes. De hoofddoelstelling van de online patrouille is om de zichtbaarheid en bereikbaarheid van de politie op internet te vergroten. Hierbij bestaat speciale aandacht voor jongeren. De politie gebruikt platforms zoals Facebook, Twitter, Instagram, en mogelijk gaming-sites waar jongeren actief zijn. Het doel is om een vertrouwensband op te bouwen met jongeren, hen te informeren over de wet en hen te adviseren over veilige online praktijken.

Daarnaast monitort de patrouille online platforms bij grote publieke evenementen, zoals concerten, sportwedstrijden of demonstraties. De politie gebruikt sociale media om de menigte te monitoren en snel te kunnen reageren op eventuele incidenten. Sociale media en andere online platforms worden ook preventief gebruikt om mogelijke dreigingen, zoals geplande gewelddadige acties of haatzaaien, vroegtijdig op te sporen. Dit stelt de politie in staat om preventieve maatregelen te nemen en mogelijk grotere incidenten te voorkomen. Hierbij mag de politie alleen gebruik maken van openbaar toegankelijke online bronnen.

¹⁶⁸ Zie ook: <https://politi.dk/national-enhed-for-saerlig-kriminalitet/nyhedsliste/politiets-online-patrouille-gaar-i-luft-en/2022/03/31>

7.4 Inzet van technische hulpmiddelen

In Denemarken maakt de politie gebruik van verschillende technologische hulpmiddelen en geavanceerde technologieën om de openbare orde te handhaven en de veiligheid te verbeteren. In deze paragraaf bespreken wij enkele van deze technische hulpmiddelen welke uit een eerste inventarisatie van documenten en literatuur naar voren zijn gekomen. Om ons uit te laten over de precieze wijze van inzet van deze technische hulpmiddelen, moeten interviews worden gehouden met de Deense politie.

Cameratoezicht

Op openbare plaatsen en in bepaalde risicogebieden maakt de Deense politie gebruik van cameratoezicht om de openbare orde te bewaken. De bevoegdheid hiervoor is neergelegd in *”Bekendtgørelse af lov om tvovervågning”* (Wet op camerabewaking). Camera’s worden ingezet bij het monitoren van grote menigten en orde verstorende incidenten snel te identificeren.

Bodycams

De Deense politie gebruikt bodycams om interacties tussen politieagenten en burgers vast te leggen. De inzet van bodycams is onderdeel van een pilot in enkele politiedistricten en de bredere inzet ervan is momenteel onderdeel van het politieke debat.

Drones

Drones worden steeds vaker door de Deense politie ingezet voor surveillance doeleinden, vooral bij grote openbare evenementen. Drones worden net zoals camera’s ingezet bij het monitoren van grote menigten en orde verstorende incidenten snel te identificeren.¹⁶⁹

Automatische nummerplaatherkenning (ANPR)

ANPR-systemen worden door de Deense politie gebruikt om voertuigen te identificeren die betrokken zijn bij misdrijven of om gestolen voertuigen op te sporen. Dit systeem kan automatisch kentekenplaten lezen van voorbijrijdende voertuigen. Het is onduidelijk in hoeverre deze methode ook wordt ingezet bij handhaving van de openbare orde.¹⁷⁰

Gezichtsherkenning

Brøndby IF, een Deense voetbalclub heeft toestemming gekregen van de Datatilsynet om gezichtsherkenningstechnologie te gebruiken. De club mag gezichtsherkenning toepassen bij het stadion om personen te identificeren. Het doel is om personen die vanwege eerdere overtredingen een stadionverbod hebben te kunnen weren, ook tijdens uitwedstrijden.¹⁷¹

Hoewel dit voorbeeld niet ziet op een politieaangelegenheid, wijst het voorbeeld erop dat gezichtsherkenning onder specifieke voorwaarden goedgekeurd kan worden door de Datatilsynet, ook voor het handhaven van de openbare orde.

¹⁶⁹ M.H. Frederiksen, J.T. Pedersen en M.T. Knudsen, *Drones for public safety and emergency response operations: Actual and planned use*, februari 2020.

¹⁷⁰ T. Kammerersgraad Christensen, *Automatisk Nummerpladegenkendelse (ANPG): – behandling af personoplysninger, proportionalitet og retten til privatlivets fred*, april 2022.

¹⁷¹ Zie: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2023/jun/broendby-if-har-faaet-lov-til-udvidet-brug-af-ansigtsgenkendelse>

7.4.1 Toezicht op technische hulpmiddelen

De Datatilsynet is verantwoordelijk voor het toezicht op de inzet van technische hulpmiddelen. De Datatilsynet kan ook adviezen uitbrengen over de inzet hiervan, zoals het geval was bij de inzet van gezichtsherkenningstechnologie bij Brøndby IF. De Deense politie heeft ook interne mechanismen om te zorgen voor de juiste toepassing van technologieën, waaronder regelmatige beoordelingen en audits.

8. Zweden

8.1 Organisatie van de openbare ordehandhaving

De handhaving van de openbare orde in Zweden vindt in samenwerking plaats tussen verschillende instanties op verschillende bestuursniveaus, met als doel de veiligheid en het welzijn van de burgers te waarborgen. De Zweedse politie is de belangrijkste wetshandhavingsinstantie in het land en heeft als primaire verantwoordelijkheid de handhaving van de openbare orde, het voorkomen en onderzoeken van misdaden, en het handhaven van de wet. De politie is verdeeld in verschillende regionale politieautoriteiten die ieder verantwoordelijk zijn voor hun eigen gebied. Zweden is opgedeeld in verschillende politiedistricten, elk onder leiding van een regionale politieautoriteit. Deze autoriteiten zijn verantwoordelijk voor het dagelijkse toezicht op de openbare orde binnen hun jurisdicties, inclusief het coördineren van reacties op noodsituaties en het handhaven van wetten en voorschriften.

Lokale politieagenten houden toezicht op specifieke gebieden en werken nauw samen met gemeenschappen om problemen aan te pakken en criminaliteit te voorkomen. Naast de politie zijn er andere wetshandhavingsinstanties in Zweden, zoals de douane (Tullverket), de nationale veiligheidsdienst (Säkerhetspolisen), en de kustwacht (Kustbevakningen). Elk van deze instanties heeft specifieke verantwoordelijkheden en bevoegdheden met betrekking tot de handhaving van de openbare orde, afhankelijk van hun respectieve mandaten. Gemeenten hebben ook een rol bij de handhaving van de openbare orde, met name op het gebied van lokale regelgeving, vergunningen en het beheer van openbare ruimte. De naleving van deze regels worden vaak gecontroleerd door gemeentelijke ordediensten. Ambtenaren van de gemeente kunnen samenwerken met de politie en andere instanties om problemen aan te pakken die de lokale gemeenschappen beïnvloeden.

8.2 Het wettelijk kader voor de uitoefening van de openbare ordetaak

Openbare ordewetgeving

De handhaving van de openbare orde in Zweden wordt gereguleerd door verschillende wetten en regelgeving die de bevoegdheden en verantwoordelijkheden van de politie en andere instanties vaststellen. Enkele belangrijke wetten die van toepassing zijn op de handhaving van de openbare orde zijn: *Polislag* (Politiewet), die de bevoegdheden van de politie regelt, de

Ordinanslag (Ordonnantiewet), *De Ordning och säkerhet* (Wet Openbare Orde en Veiligheid), die de verschillende aspecten van openbare orde en veiligheid regelt, waaronder het beheer van openbare ruimte, het houden van evenementen, de bevoegdheden van de politie om op te treden tegen verstoringen van de openbare orde, *Demonstrationlagen* (Demonstratiewet), die demonstraties en bijeenkomsten regelt, *Alkohollagen* (Alcoholwet), die het gebruik en de verkoop van alcohol reguleert, de *Polisdatalagen* (Wet politiegegevens). Deze laatste wet regelt het verzamelen, verwerken en gebruiken van gegevens door de politie. Het bepaalt de voorwaarden waaronder de politie persoonsgegevens mag verwerken en de doeleinden waarvoor deze gegevens mogen worden gebruikt. Deze wet betreft de implementatiewetgeving van EU-richtlijn 2016/680.

Uit de deskresearch zijn geen beleidsdocumenten of handleidingen naar voren gekomen die specifiek zien op het doen van online onderzoek in het kader van de handhaving van de openbare orde. Wel is er een handleiding die ziet op hoe politiemedewerkers zich dienen te uiten en te gedragen op Social Media, maar deze handleiding zegt niets specifiek over het doen van onderzoek en welke uitgangspunten daarbij dienen te worden in acht genomen.¹⁷²

De *Lagen om elektronisk kommunikation*, ook wel de 'LEK' (Elektronische communicatie Wet) regelt de elektronische communicatiesector in Zweden en kan van invloed zijn op de toegang van de politie tot communicatiegegevens, zoals internetverkeer en telecommunicatie, voor wetshandavingsdoeleinden.

Privacywaarborgen

De *Polisdatalagen* bepaalt de doelstellingen van het verzamelen en verwerken van politiegegevens, zoals het handhaven van de openbare orde, het voorkomen en bestrijden van criminaliteit, en het waarborgen van de veiligheid van individuen en de samenleving als geheel.¹⁷³ Deze wet bevat bepalingen die de rechtsgrondslag vaststellen voor de verwerking van politiegegevens. Dit omvat de voorwaarden waaronder persoonsgegevens mogen worden verzameld en verwerkt, inclusief de eisen voor rechtmatigheid, proportionaliteit en noodzakelijkheid.¹⁷⁴

Daarnaast bevat de wet bepalingen die de bescherming van persoonsgegevens waarborgen, inclusief regels voor de beveiliging en vertrouwelijkheid van politiegegevens. Deze wet bevat bepalingen die de rechten van individuen beschermen met betrekking tot hun persoonsgegevens, waaronder het recht op toegang tot hun gegevens, het recht op rectificatie en verwijdering van onjuiste of onnodige gegevens, en het recht op verzet tegen bepaalde vormen van verwerking.¹⁷⁵ Tot slot voorziet de wet onder verwijzing naar *Personuppgiftslag* in mechanismen voor toezicht en handhaving om ervoor te zorgen dat de verwerking van politiegegevens in overeenstemming is met de wet.

Over het algemeen is de *Polisdatalagen* ontworpen om een evenwicht te bieden tussen de noodzaak voor de politie om effectief op te treden tegen criminaliteit en de bescherming van de privacy en rechten van individuen.

¹⁷² Handledning Polisen i sociala medier, KA-159-3040/11.

¹⁷³ Hoofdstuk 1 Polisdatalagen

¹⁷⁴ Hoofdstuk 2 Polisdatalagen

¹⁷⁵ Hoofdstuk 3 Polisdatalagen.

8.3 Uitvoering van online informatievergaring

In Zweden voert de politie (Polisen) online informatievergaring uit ten behoeve van het handhaven van de openbare orde. Dit omvat het monitoren van sociale media, openbare fora en groepen, websites en andere online platforms om potentiële bedreigingen voor de openbare veiligheid te identificeren, zoals extremistische activiteiten, criminele gedragingen, protestbewegingen en andere relevante informatie.

Binnen de Zweedse politie zijn er verschillende speciale afdelingen en eenheden die belast zijn met inlichtingenverzameling, terrorismebestrijding, cybercriminaliteit en criminaliteitspreventie.

Cybercrime Units

Deze afdelingen zijn gespecialiseerd in het onderzoeken en bestrijden van cybercriminaliteit. Ze hebben vaak de expertise en middelen om online platforms te monitoren op criminele activiteiten, waaronder dreigingen voor de openbare orde.

Informatie- en inlichtingeneenheden

Deze afdelingen zijn verantwoordelijk voor het verzamelen, analyseren en verspreiden van informatie en inlichtingen over potentiële dreigingen voor de openbare orde. Ze kunnen online monitoring gebruiken als onderdeel van hun werk om trends en patronen te identificeren.

Regionale politieafdelingen

Binnen politieregio's kunnen specifieke afdelingen of teams belast zijn met de handhaving van de openbare orde. Deze afdelingen kunnen online monitoring gebruiken om situaties te volgen en te reageren op potentiële dreigingen.

Special Operations Units

Deze eenheden worden ingezet voor speciale operaties, waaronder crisisrespons en handhaving van de openbare orde bij grootschalige evenementen. Ze kunnen online monitoring gebruiken om de veiligheidssituatie te volgen en snel te reageren op noodsituaties.

Rechercheafdelingen

Rechercheurs kunnen online monitoring gebruiken als onderdeel van hun onderzoek naar misdaden die verband houden met de openbare orde, zoals terrorisme, extremisme of haatmisdrijven.

Verschiedende afdelingen kunnen hun expertise en middelen bundelen om een alomvattende aanpak te bieden voor het monitoren van online activiteiten en het handhaven van de openbare orde.

8.4 Inzet van technische hulpmiddelen

Cameratoezicht

De Zweedse politie gebruikt camera's om de openbare orde te handhaven. Deze camera's worden vaak geïnstalleerd op openbare plaatsen, zoals drukke straten, pleinen, stations en

andere openbare locaties, om toezicht te houden, criminaliteit te voorkomen en incidenten te onderzoeken. Verschillende wetten zijn van toepassing op het gebruik van camera's, zoals de Polislagen, de Kameraövervakningslag (Wet op cameratoezicht), de AVG en de Ordinnantiewet). Op basis van de Wet op het cameratoezicht worden technische normen gesteld aan de installatie, mogen camera's alleen gebruikt worden voor vooraf bepaalde doelen, moeten exploitanten duidelijk maken aan het publiek dat er camera's worden gebruikt. In sommige gevallen is toestemming vereist van de Zweedse Autoriteit Persoonsgegevens.

Automatische nummerplaatherkenning (ANPR)

De Zweedse politie maakt gebruik van ANPR (Automatic Number Plate Recognition) camera's voor verschillende doeleinden, waaronder het handhaven van de verkeersveiligheid, het opsporen van gestolen voertuigen, het controleren van kentekenregistraties en het handhaven van de openbare orde. Deze camera's zijn ontworpen om automatisch kentekenplaten van voertuigen te scannen en te controleren tegen databases met relevante informatie.

Net als bij andere vormen van cameratoezicht is het gebruik van ANPR-camera's onderhevig aan wet- en regelgeving met betrekking tot gegevensbescherming en privacy. De Zweedse wetgeving reguleert het gebruik van deze technologie en stelt voorwaarden vast voor het verzamelen, verwerken en opslaan van gegevens die worden verzameld door ANPR-camera's, met het oog op het waarborgen van de privacy van individuen.

Lichaamscamera's

Lichaamscamera's kunnen door de Zweedse politie worden ingezet voor verschillende doelen, zoals het verzamelen van bewijsmateriaal, het verbeteren van transparantie en verantwoording en de bescherming van politieagenten en burgers.

Drones

De Zweedse politie maakt gebruik van drones voor verschillende doeleinden, waaronder het handhaven van de openbare orde, het uitvoeren van zoek- en reddingsoperaties, het verzamelen van bewijsmateriaal bij misdrijven, en het monitoren van grote evenementen of gebeurtenissen zoals festivals en demonstraties.

Het gebruik van drones door de Zweedse politie biedt verschillende voordelen, waaronder de mogelijkheid om moeilijk bereikbare of gevaarlijke gebieden te verkennen, snel informatie te verzamelen over situaties op de grond, en om de efficiëntie en effectiviteit van politieoperaties te verbeteren.

Net als bij andere vormen van technologie en surveillance, is het gebruik van drones door de Zweedse politie onderworpen aan wet- en regelgeving met betrekking tot gegevensbescherming, privacy en luchtvaartveiligheid.

8.4.1 Toezicht op het gebruik van technische hulpmiddelen

Het toezicht op het gebruik van technische hulpmiddelen door de Zweedse politie omvat verschillende aspecten en wordt uitgevoerd door meerdere instanties en mechanismen. Enkele van de belangrijkste aspecten van dit toezicht zijn:

- Interne richtlijnen en protocollen: De Zweedse politie heeft interne richtlijnen en protocollen opgesteld die het gebruik van technische hulpmiddelen reguleren.

Verskillende externe instanties houden toezicht op het gebruik van technische hulpmiddelen door de Zweedse politie, waaronder:

- De Raad voor Bescherming van de Veiligheid en Integriteit (*Säkerhets- och integritetsskyddsnämnden*)¹⁷⁶ is belast met het toezicht op de rechtmatige verwerking van persoonsgegevens bij rechtshandhavingsactiviteiten. De toezichthoudende autoriteit op de gegevensbescherming (Integritetsskyddsmyndigheten) is de algemene toezichthoudende autoriteit. De Raad en de autoriteit hebben dezelfde taak als het gaat om het toezicht op de verwerking van persoonsgegevens door de politie.¹⁷⁷
- De Justitieombudsmannen, is een onafhankelijke overheidsinstantie die belast is met het onderzoeken van klachten over overheidsinstanties, waaronder de politie. Ze houden toezicht op de wettigheid van het handelen van overheidsinstanties en kunnen optreden als een toezichthouder op het gebruik van technische middelen door de politie.
- De Ombudsmannen van het Parlement zijn een andere toezichthoudende instantie die klachten onderzoekt over het handelen van overheidsinstanties, waaronder de politie. Ze houden toezicht op de naleving van wet- en regelgeving door overheidsinstanties en kunnen optreden als een onafhankelijke controle op het gebruik van technische middelen.
- De Luchtvaartautoriteit (Transportstyrelsen): Deze autoriteit reguleert het gebruik van drones en zorgt ervoor dat het gebruik ervan in overeenstemming is met de luchtvaartwetgeving en veiligheidsnormen.
- Rechtbanken: rechtbanken kunnen ook een rol spelen bij het toezicht op het gebruik van technische hulpmiddelen door de politie, vooral wanneer deze technologieën worden gebruikt als bewijsmateriaal in juridische procedures.
- Parlementaire controle en overheidsaansprakelijkheid: het Zweedse parlement houdt toezicht op het algemene functioneren van de politie, inclusief het gebruik van technische hulpmiddelen, door middel van parlementaire commissies en debatten. Daarnaast kunnen burgerrechtenorganisaties en de media het gebruik van technische hulpmiddelen door de politie monitoren en erover rapporteren, waardoor een vorm van externe controle en transparantie wordt geboden.

¹⁷⁶ Lag (2018:1693) om polisens behandling av personuppgifter inom brottsdatalogens område.

¹⁷⁷ Säkerhets- och integritetsskyddsnämndens, årsredovisning 2023, p. 3

9. Spanje

9.1 Organisatie van de openbare ordehandhaving

Spanje is een bondsstaat waarbij de macht voor een belangrijk deel op decentraal niveau wordt uitgevoerd. Het binnenlands bestuur bestaat uit twee autonome steden en zeventien autonome gemeenschappen. De autonome gemeenschappen zijn opgedeeld in provincies, de provincies zijn vervolgens onderverdeeld in comarca's, en ten slotte bestaan de comarca's uit verschillende gemeenten. Iedere gemeente heeft een burgemeester die verantwoordelijk is voor de openbare orde en veiligheid. De burgemeester staat in dat kader aan het hoofd van het politiekorps. De gemeenteraad stelt onder meer regelingen vast met betrekking tot de openbare orde en veiligheid.¹⁷⁸

De politie in Spanje is opgedeeld in drie korpsen: de Guardia Civil, de Policia National en de Policia Local. Er zijn ook een aantal autonome gemeenschappen (zoals Baskenland en Catalonië) die een eigen politiekorps hebben. De lokale politie houdt zich met name bezig met het verkeer, kleine openbare veiligheid verstoringen en kleine criminaliteit. De Policia National en de Guardia Civil hebben korpsen die verantwoordelijk zijn voor het van de openbare orde.¹⁷⁹

9.2 Het wettelijk kader voor de uitoefening van de openbare ordetaak

Wet 7/1985

Wet 7/1985 van 2 april 1985 regelt de inrichting van de Spaanse gemeenten. Ook worden in de wet de taken en bevoegdheden van de burgemeester genoemd. Artikel 21 bepaalt dat hij aan het hoofd staat van de lokale politie.

Organieke Politiewet 2/1986

De *organieke Politiewet 2* van 1986 regelt de basisstructuur, functies en werking van de verschillende politiediensten in Spanje, waaronder de Nationale Politie, de Guardia Civil, en de regionale en lokale politiekorpsen. De bevoegdheden van de politie zijn daarin ook vastgelegd. De wet bevat ook principes die gelden voor de politie, zoals het principe dat inzet van bevoegdheden proportioneel moet zijn. Over het verzamelen van data is in hoofdstuk artikel 11

¹⁷⁸ Cachet e.a., Buitenlandse burgemeesters bekeken, 2002, <https://repub.eur.nl/pub/1119/CLD005.pdf>.

¹⁷⁹ <https://polis.osce.org/country-profiles/spain>.

van hoofdstuk twee van de wet onder meer vastgelegd dat de politie gegevens mag vastleggen, ontvangen en analyseren die van belang zijn voor het handhaven van de openbare orde en veiligheid.

Organieke wet 7/2021

De organieke wet 7/2021 is de Spaanse uitvoeringswet van de AVG en de implementatiewet van de EU-richtlijn 2016/680.

Organieke Wet 4/2015

Deze wet reguleert de maatregelen die de politie kan nemen om de openbare veiligheid te handhaven en stelt sancties vast voor handelingen die als verstoringen van de openbare orde worden beschouwd.

Wetgeving voor het doen van online onderzoek i.h.k. openbare orde handhaving

In Spanje is geen specifieke wetgeving voor het doen van online onderzoek door de politie in het kader van de openbare orde handhaving. Als het gaat over onderzoek op het gebied van het strafrecht is er wel specifieke wetgeving over de politiebevoegdheden. De geïnterviewde uit Spanje geeft aan dat er juridisch gezien geen belemmeringen zijn informatie op internet, zoals social media te vergaren in het kader van de handhaving van de openbare orde. Daarbij moet echter wel worden voldaan aan de voorwaarden van de Organieke wet 7/2021.

9.3 De uitvoering van online informatievergaring

Onze gesprekspartner in Spanje geeft aan dat de politie in Spanje gebruik maakt van informatie op bijvoorbeeld social media in het kader van de openbare orde handhaving. Hij kende onder meer een voorbeeld waarbij hooligans gesprekken voerden via Twitter and de politie door het screenen en lezen van die berichten kon ingrijpen. Hij weet niet in welke mate er gebruik wordt gemaakt van het zoeken publiek toegankelijke informatie, maar geeft aan dat het wel wordt gedaan.

9.4 Inzet van technische hulpmiddelen

Automatische nummerplaatherkenning (ANPR)

Automatische nummerplaatherkenning (ANPR) wordt in Spanje ingezet om de verkeersveiligheid te waarborgen.

Drones

Daarnaast gebruikt de politie drones om de openbare orde te handhaven. Deze onbemande apparaten worden gebruikt om mensenmassa's in de gaten te houden tijdens openbare evenementen, protesten en demonstraties. Door potentiële bedreigingen op te sporen en aanstichters te identificeren, kunnen drones de ordehandhavers helpen geweldsuitbarstingen te voorkomen en de openbare veiligheid te waarborgen.¹⁸⁰

Lichaamscamera's

In Spanje wordt ook gebruik gemaakt van lichaamscamera's. Aanleiding hiervoor waren de toename van fysieke agressie richting agenten en de klachten en publieke beschuldigingen

¹⁸⁰ <https://aerialproductions.es/drones-servicio-policial/>.

waarmee de politie te maken krijgt bij de inzet van geweld. De beelden van de lichaamscamera's kunnen worden gebruikt bij eventuele rechtszaken over de inzet van geweld.¹⁸¹

Cameratoezicht

Cameratoezicht wordt in Spanje ook ingezet en is geregeld in de Organieke wet nr. 4/1997. Deze wet staat het gebruik van camera's toe voor de openbare veiligheid en de bescherming van de openbare orde, wanneer dit strikt noodzakelijk is en bepaalde waarborgen met betrekking tot rechten van derden in acht worden genomen.¹⁸²

In de wet voor het gebruik van camera's wordt onderscheid gemaakt tussen het gebruik van vaste camera's en het gebruik van mobiele camera's. Voor het gebruik van vaste camera's in openbare ruimten is voorafgaand toestemming nodig van de gouverneur van de provincie.

Daarnaast is een oordeel vereist van een speciale commissie bestaande uit de voorzitter van het provinciale gerechtshof, een vertegenwoordiger van de nationale regering, een procureur-generaal en een burgemeester. Voor de inzet van mobiele camera's moet er goedkeuring zijn van het hoofd van de politie. Daarvoor is vooraf geen advies van de commissie vereist. De commissie houdt wel toezicht op de toepassing en het gebruik van de opnames door de mobiele camera's.¹⁸³

¹⁸¹ <https://www.elconfidencialdigital.com/articulo/seguridad/interior-adquiere-nueva-partida-camaras-unipersonales-policias-plena-polemica-agresiones-agentes/20230905172015631140.html>.

¹⁸² Zie <https://zoek.officielebekendmakingen.nl/nds-bzk0300082-b1.pdf>, p. 22.

¹⁸³ <https://zoek.officielebekendmakingen.nl/nds-bzk0300082-b1.pdf>, p. 22.

10. Conclusies

Het doel van dit onderzoek was een verkenning van de vormgeving van buitenlandse stelsels, de mate waarin deze rechtmatig en effectief zijn en de inspiratie die dat voor de Nederlandse wetgever zou kunnen bieden bij het vormgeven van nieuwe wetgeving die de politie expliciete bevoegdheden moet verschaffen om online onderzoek te doen in publiek toegankelijke bronnen bij openbare ordeverstoringen. Zoals we in hoofdstuk 1.6 hebben aangegeven hebben we de laatste twee hoofdvragen niet kunnen beantwoorden. We hebben niet kunnen vaststellen hoe bevoegdheden in de praktijk werken. Het onderzoek beperkt zich dus tot een beschrijving van het wettelijke stelsel in een aantal Europese landen voor het door de politie verzamelen van (online) gegevens ten behoeve van de openbare ordetaak en de actoren die daarbij betrokken zijn. Hieronder worden de belangrijkste bevindingen nogmaals in hoofdlijnen weergegeven.

10.1 Bevindingen

In geen van de onderzochte landen hebben we expliciete bevoegdheden aangetroffen voor het online vergaren van persoonsgegevens uit publiek toegankelijke bronnen ten behoeve van de openbare ordetaak. Wel zien we in de onderzochte landen wettelijke kaders waarin die bevoegdheden worden ontleend aan meer algemeen geformuleerde bepalingen. Ook zien we verschillen en overeenkomsten tussen landen in de manier waarop het stelsel omtrent openbare orde bevoegdheden is vormgegeven en hoe het toezicht op de uitoefening van die bevoegdheden is georganiseerd. We beperken ons hier tot Frankrijk, Engeland, België en Duitsland waarover we de meeste informatie hebben kunnen verzamelen.

10.1.1 Frankrijk en Engeland: één integraal wettelijk kader, één toezichthouder

We zien dat in Frankrijk en Engeland in de basis vergelijkbare stelsels bestaan. Deze stelsels vinden hun oorsprong in gebeurtenissen die een grote maatschappelijke impact hebben gehad en die hebben geleid tot wetswijzigingen. Voor Engeland zijn dat de London Riots geweest in 2011 en in Frankrijk was dat de aanslag op Charlie Hebdo en de aanslag op de Bataclan in Parijs in 2015.

In zowel Frankrijk als Engeland zijn overkoepelende wetten geïntroduceerd die de bevoegdheden regelen voor alle diensten met intelligencebevoegdheden. In Frankrijk werd in 2015 de Loi relative au renseignement (Wet op de inlichtingen) aangenomen. De wet regelt het gebruik van bijzondere bevoegdheden voor gegevensvergaring, zowel door inlichtingen- als

politiediensten, in het kader van nationale veiligheid en openbare orde. Denk hierbij aan observatie, en toegang tot elektronische communicatie. In de wet wordt een limitatief aantal doelen omschreven waarvoor het vergaren van informatie is toegestaan. Het toezicht wordt in Frankrijk uitgeoefend door de Commission nationale de contrôle des techniques de renseignement (CNCTR), een onafhankelijke toezichthouder met juridische, parlementaire en technische expertise. De CNCTR moet vooraf advies uitbrengen over het gebruik van bevoegdheden en controleert ook de naleving achteraf.

In Engeland werd het versnipperde wettelijke kader vervangen door de Investigatory Powers Act (IPA) in 2016. De IPA bundelt vrijwel alle bevoegdheden tot gegevensvergaring – inclusief interceptie, metadata-analyse, en toegang tot communicatie-inhoud – in één wettelijk kader. De wet geldt niet alleen voor politiediensten, maar ook voor veiligheids- en inlichtingendiensten, en legt per bevoegdheid vast welke instantie deze mag gebruiken, onder welke voorwaarden, en met welke procedurele waarborgen. Centraal in het stelsel staat de Investigatory Powers Commissioner's Office (IPCO), een onafhankelijk toezichthoudend orgaan dat bestaat uit (oud-)rechters en deskundigen. Het IPCO houdt toezicht op de rechtmatigheid van het gebruik van bevoegdheden, voert audits uit, en rapporteert jaarlijks aan het parlement. Voor veel bevoegdheden is voorafgaande goedkeuring van zowel een minister als een rechter vereist.

Zowel Frankrijk als Engeland combineren een integrale wettelijke basis met onafhankelijke en gespecialiseerde toezichtmechanismen (CNCTR en IPCO) die als buffer dienen tussen uitvoerende macht en burgerrechten.

Opvallend is dat deze stelsels gelijkenissen vertonen met de wijze waarop in Nederland het wettelijk kader en de governance rondom de inlichtingendiensten is georganiseerd; één wet waarin de bevoegdheden zijn georganiseerd en een specifieke toezichthouder die toezicht houdt op de inzet van de bevoegdheden die aan de wet kunnen worden ontleend. Het belangrijke verschil met Frankrijk en Engeland is dat in deze landen dat stelsel voor alle autoriteiten met gegevensvergarende bevoegdheden geldt; alle autoriteiten ontleen deze bevoegdheden aan één wet en zijn onderworpen aan een en dezelfde toezichthouder.

10.1.2 Duitsland: bevoegdheden voor openbare ordetaken voornamelijk op deelstaat-niveau, belangrijke rol voor rechterlijke toetsing

In Duitsland is het wettelijke kader voor het verzamelen van persoonsgegevens door de politie federatief georganiseerd. Dat betekent dat zowel de Bondsregering als de deelstaten (Länder) eigen bevoegdheden en wetgeving hebben. De federale politie (Bundespolizei) en de inlichtingendienst (Bundesnachrichtendienst, BND) vallen onder het gezag van de federale overheid en opereren op basis van federale wetten, zoals de Bundespolizeigesetz en de Gesetz über das Bundeskriminalamt (BKAG). Tegelijkertijd hebben de zestien deelstaten elk hun eigen politieorganisaties en -wetten.

Voor gegevensverzameling in het kader van openbare orde en veiligheid zijn vooral de deelstaatpolitieën verantwoordelijk. Zij opereren op basis van eigen politiewetten (Polizeigesetze), waarin bevoegdheden omtrent gegevensvergaring zijn geregeld. Hierdoor kunnen de regels per deelstaat verschillen, al zijn ze allemaal gebonden aan het Grundgesetz (de Duitse Grondwet) en het federale kader van grondrechten en jurisprudentie.

De rechterlijke toetsing speelt in Duitsland een centrale rol. Veel vormen van gegevensverzameling, zeker de ingrijpende, vereisen voorafgaande rechterlijke toestemming. Dit is bijvoorbeeld het geval bij surveilleren in besloten groepen op het internet. Daarnaast is het Bundesverfassungsgericht (het Federale Constitutionele Hof) een belangrijke actor: het heeft in verschillende baanbrekende uitspraken strenge eisen gesteld aan rechtmatigheid, proportionaliteit, transparantie en rechtsbescherming bij gegevensverzameling. Een belangrijke uitspraak is bijvoorbeeld de uitspraak van 16 februari 2023, waarbij is bepaald dat het geautomatiseerd verwerken en analyseren van persoonsgegevens met behulp van grootschalige geautomatiseerde verwerking in strijd is met het recht op informationele zelfbeschikking.

Het toezicht op inlichtingendiensten en politietaken ligt deels bij onafhankelijke commissies, zoals de G10-commissie (voor communicatie-interceptie), en bij externe toezichthouders op zowel federaal als deelstaatsniveau.

10.1.3 **België: geen specifieke grondslag voor het doen van online onderzoek**

In België is het bewaren of herstellen van de openbare orde en veiligheid primair een verantwoordelijkheid van de burgemeester. Die verantwoordelijkheid strekt zich uit over de inzet van de bestuurlijke politie op het grondgebied van de gemeente. Het optreden van de bestuurlijke politie kenmerkt zich vooral door het preventieve karakter, waarbij het met name gaat om door middel van preventieve maatregelen verstoring van de openbare orde te voorkomen.

De bestuurlijke politie maakt in dat kader gebruik van online onderzoek. De werkwijze op dat vlak loopt tussen de politiezones sterk uiteen. Uit de literatuur volgt dat vooral niet-geautomatiseerd online onderzoek in openbare bronnen plaatsvindt. Het gebruik van geautomatiseerde vormen van online onderzoek is minder breed verspreid.

De burgemeester en de bestuurlijke politie opereren op basis van de Nieuwe Gemeentewet en de Wet op het politieambt (Wpa), waarbij de Wpa een meer algemene basis biedt voor het verzamelen van persoonsgegevens door de politie. De Wpa voorziet echter niet in een specifieke grondslag voor het doen van online onderzoek. Een eerder voorstel tot uitbreiding van artikel 26 Wpa, waarin – kort gezegd – het betreden van publieke plaatsen is geregeld, is uiteindelijk niet ingevoerd.

Ondanks dat artikel 26 Wpa niet is uitgebreid tot online onderzoek volgt uit het Agora-arrest van het Hof van Cassatie dat artikel 26 Wpa een grondslag biedt voor het betreden van online publiek toegankelijke plaatsen door de politie. Het gebruik van een alias kan daarbij onder voorwaarden behoren tot de normale wijze van het bezoeken van delen van het internet door de politie.

Het toezicht bestaat uit intern toezicht binnen de politie, maar ook uit extern toezicht door toezichthouders als de Algemene inspectie, Comité P en Het Controleorgaan op de Politie Informatie.

Regels voor de inzet en het gebruik van bewakingscamera's zijn vastgelegd in verschillende regelingen. Zo is er onder meer wetgeving in het gebruik van bijzondere opsporingsmethodes, voor bewakingscamera's in het algemeen en voor bewakingscamera's in voetbalstadions. Het gebruik van camera's door de politie wordt geregeld door de Wpa. Camera's van andere partijen zoals steden en gemeenten worden geregeld door de Camerawet.

TABEL 10.1 SAMENVATTING BEVINDINGEN

	Deelonderzoek B				Deelonderzoek A			
	Frankrijk	Engeland	Duits-land/Hes-sen	België	Ierland	Dene-marken	Zweden	Spanje
Wettelijk onderscheid openbare orde en strafrecht/opsporing	Nee	Nee	Ja	Ja	Ja	Ja	Ja	Nee
Online gegevensvergaring bij handhaving openbare orde	Ja	Ja	ja	Ja	Ja	Ja	Ja	Ja
Specifieke wettelijke bevoegdheid voor online gegevensvergaring	Nee	Nee	Nee	Nee	Nee	Nee	Nee	Nee
Beleid/richtlijnen aange-troffen voor online gege-vensvergaring	Nee	Ja	Ja	Nee	Ja	Nee	Nee	Nee
Actor die online gegevens verzamelt	Verschil-lende	Verschil-lende	Politie	Politie	Verschil-lende	Politie	Politie	Politie

10.2 Slotbeschouwing

In geen van de onderzochte landen is sprake van een specifieke wettelijke grondslag die expliciet voorziet in online gegevensvergaring ten behoeve van de handhaving van de openbare orde – zoals die in Nederland momenteel in voorbereiding is (zie consultatievoorstel van Regels over gegevensvergaring voor de handhaving van de openbare orde (Wet gegevensvergaring openbare orde) van 2025¹⁸⁴). Bevoegdheden voor dergelijke vormen van informatievergaring worden doorgaans afgeleid uit bredere wettelijke kaders, zoals politiewetten of wetten op de inlichtingendiensten.

Toch zien we dat in alle onderzochte landen – zij het in verschillende mate – het doen van online onderzoeken al sinds het ontstaan van de mogelijkheden voor het doen van online onderzoek onderwerp is van maatschappelijk debat. Het gaat hierbij over de toelaatbaarheid van online onderzoek door de politie, met name wanneer het gaat om het betreden van besloten digitale omgevingen, het gebruik van geautomatiseerde analysemiddelen of het standaard volgen van burgers op sociale media e.d.

In sommige gevallen worden de grenzen opgezocht, wat resulteert in kaderstellende jurisprudentie. Zo heeft het Duitse Bundesverfassungsgericht in februari 2023 geoordeeld dat groot-schalige geautomatiseerde analyse van persoonsgegevens door de politie in strijd is met het grondrecht op informationele zelfbeschikking. Hierbij wordt opgemerkt dat deze uitspraak niet specifiek zag op het doen van online onderzoek. Ook in België heeft het Hof van Cassatie zich uitgesproken over de voorwaarden waaronder de politie online onderzoek mag doen met behulp van nepprofielen. In de Agora-zaak oordeelde het Hof dat het gebruik van een fictief

¹⁸⁴ [Overheid.nl | Consultatie Wet gegevensvergaring openbare orde](#)

profiel in principe is toegestaan, mits het profiel geen bestaande persoon imiteert en er geen sprake is van misleiding. Daarnaast bevestigde het Hof dat informatie op sociale media als openbaar kan gelden als gebruikers daarvoor uitgenodigd zijn, zoals bij besloten Facebook-groepen.

Dit onderzoek laat zien dat ook in anderen landen discussie bestaat over hoe ver de politie mag gaan bij online gegevensvergaring en het volgen van burgers via internet. Er ontbreken in de bestudeerde landen specifieke wettelijke bepalingen voor het doen van online onderzoeken met het oog op het handhaven van de openbare orde.

Bijlage 1: Geraadpleegde bronnen

Frankrijk

7^e Rapport d'activité 2022

CNCTR, *7^e Rapport d'activité*, 2022.

8^e Rapport d'activité 2023

CNCTR, *8^e Rapport d'activité*, 2023.

Agence de développement et d'urbanisme de Lille Métropole 2021

l'Agence de développement et d'urbanisme de Lille Métropole, *Grensoverschrijdende samenwerking en territoriale organisatie in Frankrijk en België*, 2021.

Auffret & Durand 2019

S. Auffret & A.A. Durand, 'CRS, gendarmes mobiles, BRAV... quelles sont les sept familles des forces de l'ordre?', *lemonde.fr*, 4 mei 2019.

CNIL 2015

CNIL, *Délibération n° 2015-078 du 5 mars portant avis sur un projet de loi relative au renseignement*, 2015.

Maillet-Contoz 2018

J. Maillet-Contoz, *Terrorism and Counterterrorism: French Policy after the 2015 Attacks*, 2018.

Mendiboure 2021

D. Mendiboure, 'Quelles sont les différences entre la police nationale et la police municipale?', Ministère de l'intérieur (online).

Noordegraaf e.a. 2017

M. Noordegraaf e.a., *Nood breekt wet? Terroristische dreiging, noodtoestand en maatschappelijke effecten*, WODC, 2017.

Urvoas & Verchère 2013

J.J. Urvoas & P. Verchère, *Rapport d'information déposé en application de l'article 145 du Règlement par la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République, en conclusion des travaux d'une mission d'information sur l'évaluation du cadre juridique applicable aux services de renseignement, et présenté*, 2013.

Engeland

Egawhary 2019

E.M. Egawhary, *'The Surveillance Dimensions of the Use of Social Media by UK Police Forces'*, 2019.

Home Office 2018

Home Office, *Covert Surveillance and Property Interference: Revised Code of Practice*, August 2018.

Lancaster City Council 2018

Lancaster City Council, *The Regulation of Investigatory powers act (RIPA) Policy and procedure*, 2018.

Lloyd 2019

P. Lloyd, *'Internet Intelligence & Investigations Strategy'*, NPCC, 2019.

Privacy International 2020

Privacy International, *Is your Local Authority looking at your Facebook likes?*, 2020.

Duitsland, deelstaat Hessen

Bijleveld e.a. 2021

C. Bijleveld e.a., *'Politiefunctie in een veranderende omgeving'*, WRR, 2021.

Rogier e.a. 2002

L.J.J. Rogier e.a. *'Handhaving van de openbare orde in het buitenland: overzicht van bevoegdheden en praktische toepassing en toepasbaarheid in Nederland'*, 2002.

WRR 2021

WRR, *Appendix D North Rhine-Westphalia/Germany*, 2021.

België

Bijleveld e.a. 2021

C. Bijleveld e.a., *'Politiefunctie in een veranderende omgeving'*, WRR, 2021.

Cachet 2002

A. Cachet e.a. *'Buitenlandse Burgemeesters Bekeken'*, CLD, 2002.

Clerix 2023

K. Clerix, *'Online patrouilleren: wat de politie wél en niet mag'*, knack.be, 4 juli 2023.

Commissie voor de bescherming van de persoonlijke levenssfeer 2016

Commissie voor de bescherming van de persoonlijke levenssfeer, *Advies over het voorontwerp van wet betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties*, mei 2016.

Conings & Van Linthout 2012

C. Conings & P. van Linthout, *'Sociale media, een nieuwe uitdaging voor politie en justitie'*, *Panopticon* 2012, afl. 3, p. 205-230.

De Wolf 2023

L. de Wolf, *'Na berichten dat illegale raveparty op til was: Kanne bij Riemst tijdelang afgesloten, twee arrestaties'*, vrt.be, 4 augustus 2023.

Federale Overheidsdienst Binnenlandse Zaken 2025

Federale Overheidsdienst Binnenlandse Zaken, *ministeriële omzendbrief OOP 41bis*

betreffende operationalisering van het referentiekader CP 4bis over het genegotieerd beheer van de openbare ruimte, januari 2025.

Moor 2020

L.G. Moor, *Cahiers Politiestudies jaargang 2020-2. Toezicht op de politie*, Gompel&Svacina, Nr. 55, 2020.

Rogier 2002

L.J.J. Rogier e.a. *‘Handhaving van de openbare orde in het buitenland: overzicht van bevoegdheden en praktische toepassing en toepasbaarheid in Nederland*, 2002.

Saelens 2022

R. Saelens, ‘De wet op het politieambt en technologische ontwikkelingen: de focus op internet patrouilleren in het kader van de bestuurlijke politie’ in: F. Goossens, K. de Pauw & F. Verspeelt (red.), *De sluier rond anonimiteit opgelicht...*, Brugge: Die Keure, 2022, p.385-392.

Schram 2022

F. Schram, ‘De camerawetgeving en haar actuele betekenis voor de lokale en federale politie’ in: F. Goossens, K. de Pauw & F. Verspeelt (red.), *De sluier rond anonimiteit opgelicht...*, Brugge: Die Keure, 2022, p. 254-256.

Todts 2024

L. Todts, ‘De gemeentelijke bestuurlijke handhaving van ondermijnende criminaliteit: naar een (lokaal) bestuursstrafrecht?’, *Tijdschrift voor Gemeenterecht (Brussel)*, p. 142-164, 2024.

Van Biervliet, Maesschalck & Rooseleers 2024

D. van Biervliet, J. Maesschalck & L. Rooseleers, ‘Technologie in de Belgische lokale politie: Ee bredere verspreiding?’, *Panopticon* 2024, afl. 5.

Van Robaey 2018

P. van Robaey, *‘Online drugshandel op het darknet: Van het indommelen van de wetgever tot de online infiltratie’*, 2018.

Vandevoorde 2019

M. Vandevoorde, *‘De bevoegdheden van de Burgemeester in tijden van Radicalisering’*, 2018.

Vanmeldert 2021

D. Vanmeldert, ‘Steeds meer camera's in het straatbeeld: "Ze voorkomen criminaliteit niet, de samenleving wordt er niet beter van"’, vrt.be, 25 maart 2021.

Vast Comité van Toezicht op de politiediensten 2022

Vast Comité van Toezicht op de politiediensten, *Het functioneren van de geïntegreerde politie inzake ANPR-hit-afhandeling van gestolen nummerplaten*, 2022, h. 5.

Wauters e.a. 2021

E. Wauters e.a., *Rapport over bevoegdheden in het delen van gegevens. Automatische kentekenplaatherkenning (ANPR) als toepassingsgeval*, Kenniscentrum Data & Maatschappij, februari 2021.

Winter e.a. 2020

H. Winter e.a., *De verwerking van politiegegevens in vijf Europese landen*, WODC, 2020.

Ierland

Garda Síochána 2023

Garda Síochána, *Open Source Intelligence Policy Document*, januari 2023, p.2.

Garda Síochána 2022

Garda Síochána, *Garda Decision Making Model Policy Document*, december 2022 p. 4-7.

Garda Síochána 2018

Garda Síochána, *The future of policing in Ireland*, september 2018.

Garda Síochána z.d.

Garda Síochána, *Connect. An Garda Síochána Digital Strategy 2019-2023*, z.d.

Denemarken

Christensen 2022

T.K. Christensen, 'Automatisk Nummerpladegenkendelse (ANPG): – behandling af personoplysninger, proportionalitet og retten til privatlivets fred', *Nordisk Tidsskrift for Kriminalvidenskab*, 2022, 271-287.

Frederiksen, Pedersen & Knudsen 2020

M.H. Frederiksen, J.T. Pedersen & M.P. Knudsen, *Drones for public safety and emergency response operations: Actual and planned use*, SDU, 2020.

Zweden

Rikspolisstyrelsen 2014

Rikspolisstyrelsen, '*Handledning Polisen i sociala medier*', 2014.

Spanje

Cachet 2002

A. Cachet e.a. '*Buitenlandse Burgemeesters Bekeken*', CLD, 2002.

Lanau z.d.

R. Lanau, '*Drones para el servicio policial*', aerialproductions.es, z.d.

Rogier e.a. 2002

L.J.J. Rogier e.a. '*Handhaving van de openbare orde in het buitenland: overzicht van bevoegdheden en praktische toepassing en toepasbaarheid in Nederland*, 2002, p.22.

Bijlage 2: Lijst van gesprekspartners

j

Nederland

- Adviseur Intelligence Korpsleiding Nationale Politie
- Landelijk portefeuillehouder Intelligence Nationale Politie
- Strategisch adviseur Intelligence Nationale Politie

Frankrijk

- Beleidsmedewerker Nederlandse ambassade in Parijs

Engeland

- Professor of law, Manchester University

Duitsland

- Junior Professor criminologie, Ruhr-Universiteit Bochum
- Hoogleraar, Duitse Politie Universiteit
- Beleidsmedewerker, Federal Commissioner for Data Protection and Freedom of Information

België

- Professor bestuursrecht, Universiteit Gent
- Commissaris-onderzoeker, Controleorgaan op de politionele informatie en vrijwillig wetenschappelijk medewerker, Vrije Universiteit Brussel
- Promovendus, Leuvens Instituut voor Criminologie, Katholieke Universiteit Leuven

Denemarken

- Assistent Professor, Universiteit Kopenhagen

Spanje

- Postdoctoraal onderzoeker, Rijksuniversiteit Groningen

pro facto