HOOGHIEMSTRA & PARTNERS
strategisch en juridisch advies

pro facto

Internationale verkenning bevoegdheden

Bewaken en beveiligen

Colofon

Hooghiemstra & Partners
Bezuidenhoutseweg 161
2594AG Den Haag
www.hooghiemstra-en-partners.nl
info@hooghiemstra-en-partners.nl

Dit onderzoek is – in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum – uitgevoerd door Hooghiemstra & Partners, strategisch en juridisch adviesbureau op het raakvlak van data en recht en Pro Facto, bureau voor bestuurskundig en juridisch onderzoek.

Auteurs: Thijs Drouen, Anna Keuning, Lieve Smeets (Hooghiemstra & Partners)
Heinrich Winter, Christian Boxum, Stan Roggeveen (Pro Facto)

Opdrachtgever: Wetenschappelijk Onderzoek- en Datacentrum (WODC)

Datum: 18 december 2025

Begeleidingscommissie:

Prof. dr. mr. G.K. Sluiter (Voorzitter, UvA)
Dr. I.W.J. van der Vegt (UU)
Dr. E. de Busser (UvA)
Drs. P.S.M. Rademakers, opgevolgd door mw. C.E. Stokhof (MinJenV)
Mr. W.M de Jongste (WODC)

Foto credit voorblad:

Bosco Yun via Unsplash

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.

Inhoud

Afkortingenlijst

ADIV	Algemene Dienst Inlichting en Veiligheid
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AVG	Algemene Verordening Gegevensbescherming
BKA	Bundeskriminalamt
CITCO	Centro de Inteligencia contra el Terorrisme y el Crimen Organizado
CNCTR	Commission nationale de contrôle des techniques de renseignement
CNI	Centro Nacional de Inteligencia
COPASIR	Comitato parlamentare per la sicurezza della Repubblica
DGSI	Direction générale de la sécurité intérieure
DJO	Directie van de operaties inzake gerechtelijke politie
EHRM	Europees Hof van de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
FE	Forsvarets Efterretningstjeneste
IVBPR	Internationaal Verdrag inzake burgerrechten en politieke rechten
KMar	Koninklijke Marechaussee
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MPS	Metropolitan Police Service
NCCN	Nationaal Crisiscentrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
OM	Openbaar Ministerie
OVV	Onderzoeksraad voor Veiligheid
RaSP	Royalty and Specialist Protection
PET	Politiets Efterretningstjeneste
SDLP	Service de La Protection
Stelsel B&B	Stelsel van Bewaken & Beveiligen
UCIS	Ufficio centrale interforze per la Sicurezza personale
UCLAT	Unité de Coordination de la Lutte Antiterroriste
Vast Comité I	Vast Comité van Toezicht op de inlichtingendiensten
Vast Comité P	Vast Comité van Toezicht op de politiediensten

Samenvatting

Inleiding

In dit onderzoek is het stelsel van bewaken en beveiligen in een aantal Europese landen onderzocht. Het doel van het onderzoek is om inspiratie te bieden voor de doorontwikkeling van het Nederlandse stelsel van bewaken en beveiligen. In het onderzoek is in het bijzonder ingegaan op de vraag hoe in de onderzochte landen het verzamelen en delen van informatie is geregeld om bedreigde personen te kunnen beveiligen. Op basis van de bevindingen uit de onderzochte landen is een raamwerk gecreëerd die toont hoe een adequaat stelsel van bewaken en beveiligen eruit kan zien. Hierbij is gebruik gemaakt van verschillende elementen van de stelsels in de onderzochte landen. Daarbij is het van belang op te merken dat de elementen uit deze stelsels niet los kunnen worden gezien van de context van het stelsel waaruit ze zijn afgeleid. Het onderzoek kan voor Nederland als inspiratie dienen voor de manier waarop de coördinerende rol binnen de verschillende stelsels is ingericht, de wijze waarop casusoverleggen worden gehouden en de wijze waarop (dwang)bevoegdheden bij wet zijn geregeld.

Aanleiding

Nederland is in de afgelopen jaren opgeschud door verschillende (zware) geweldsincidenten gericht tegen personen. Deze aanslagen hebben grote invloed op de democratische rechtsstaat en (het gevoel van) veiligheid en vrijheid. Met het stelsel bewaken en beveiligen (hierna: B&B) geeft de overheid uitvoering aan haar zorgplicht om burgers tegen (levens)gevaar te beschermen. Het stelsel staat onder druk en er wordt steeds meer van gevraagd door een stijgende hoeveelheid dreigingen. De afgelopen jaren zijn er verschillende onderzoeken gedaan naar de werking van het stelsel van B&B uitgevoerd. De uitkomsten van deze onderzoeken hebben ertoe geleid dat het stelsel van B&B in 2023 herzien is. Een specifiek belangrijk punt hierbij is de grondslag en daarbij horende knelpunten omtrent het uitwisselen en verzamelen van informatie in beveiligingssituaties. Het Wetenschappelijk Onderzoek- en Datacentrum (hierna: WODC) heeft gevraagd een rechtsvergelijkend onderzoek uit te voeren naar het bewaken en beveiligen van personen in een aantal Europese landen.

Het stelsel van bewaken en beveiligen in Nederland

Het Nederlandse stelsel van B&B is een samenwerking tussen NCTV, OM, politie, KMar, AIVD, MIVD en burgemeesters. Hoewel er geen specifieke wettelijke grondslag voor het samenwerkingsverband bestaat, zijn procedures en verantwoordelijkheden vastgelegd in de Circulaire Bewaken en Beveiligen. Het stelsel bepaalt hoe dreiging en risico-informatie leiden tot beveiligingsmaatregelen en wie deze uitvoert, waarbij de minister van Justitie en Veiligheid (JenV) eindverantwoordelijk is. Veiligheid is een gedeelde verantwoordelijkheid van overheid, burgers en werkgevers, waarbij de overheid pas ingrijpt wanneer anderen onvoldoende bescherming kunnen bieden. Decentraal gezag speelt een centrale rol, maar het Rijk heeft een bijzondere verantwoordelijkheid voor aangewezen personen, objecten en diensten. Dreigingsanalyses worden opgesteld door AIVD, MIVD en politie, terwijl politie en KMar de beveiliging uitvoeren onder regie van de minister via de NCTV.

Er is in Nederland geen wettelijke grondslag voor het samenwerkingsverband waarop het stelsel van B&B is gebaseerd. De taken die uit het stelsel voortvloeien zijn bij wet toebedeeld aan de minister van JenV en de politie. Taken die door de politie (en de KMar) worden uitgevoerd zijn vastgelegd in de Politiewet. Bevoegdheden in het kader van B&B zijn beperkt tot de algemene taakstelling van de politie

waarbij een ‘niet meer dan geringe inbreuk’ op de persoonlijke levenssfeer mag worden gemaakt. Door deze beperkingen kan de politie geen diepgaand onderzoek verrichten en kunnen dreigingen blijven bestaan zonder in beeld te komen bij de opsporingsdiensten. Wanneer dus geen strafvorderlijke middelen of bijzondere wetten van toepassing zijn voor de politie om gegevens te verzamelen en onderzoek te doen, kan alleen op basis van de algemene taakstelling informatie worden vergaard. Dit leidt tot problemen wanneer vanuit het perspectief van de bedreiger (een persoon of groepering) informatie moet worden verzameld om een concrete dreiging en de modus operandi te detecteren en wanneer vanuit het perspectief van de bedreigde persoon informatie moet worden verzameld om de (potentiële) dreigingen te detecteren en te analyseren. Ook blijkt dat de verschillende samenwerkingspartners te veel verkokerd werken wat ten koste gaat het opstellen van adequate risicobeoordelingen en het treffen van passende beveiligingsmaatregelen.

Onderzoeksvragen

De volgende onderzoeksvragen staan centraal in dit rapport. Deze luiden (verkort weergegeven):

1. Hoe is het bewaken en beveiligen van personen in een aantal EU-landen organisatorisch vormgegeven?
2. Wat is in de geselecteerde landen het juridisch kader voor de informatieverzameling en informatiedeling met betrekking tot het bewaken en beveiligen van personen?
3. Op welke wijze is een externe toetsing geregeld?
5. Is in de geselecteerde landen (wetenschappelijk) onderzoek verricht naar de toepassing van de daar geregelde bevoegdheden in de praktijk?
6. Wat is er uit de praktijk van de geselecteerde landen te leren over het verzamelen en delen van informatie?
7. Welke elementen uit de onderzochte landen kunnen ter inspiratie dienen voor het Nederlandse stelsel van B&B?

Onderzoeksaanpak

De focus van het onderzoek ligt primair op personen die bedreigd worden door terrorisme en georganiseerde misdaad omdat tijdens de onderzoeksperiode is gebleken dat deze dreigingen het meest bepalend zijn voor de werking van de verschillende systemen en daarmee de meest bruikbare informatie opleveren. Dat betekent dat de focus minder gericht is op de bescherming van (kroon)getuigen en VIPS. Dreigingen in de familiaire of relationele sfeer vallen buiten de scope van dit onderzoek.

Voor de selectie van te onderzoeken landen is een aantal randvoorwaarden geformuleerd:

- Het land ligt binnen de rechtsmacht van het EVRM;
- Er is sprake van een juridisch kader en (een vorm van) gezag en toezicht;
- De bevoegdheid tot bewaken en beveiligen van personen omvat in ieder geval het (online) verzamelen van gegevens;
- De informatie is zonder bovenmatige inspanningen te vinden.

Naast deze randvoorwaarden is een aantal aanvullende kenmerken/criteria geformuleerd om tot een gevarieerde selectie van landen te komen. Er is gelet op:

- Ordening van de veiligheids- en politiestructuur;
- Aard van het rechtsstelsel;
- Culturele en maatschappelijke perceptie van veiligheid;
- Aanwezigheid internationale instellingen;
- Historische context en ervaringen met dreigingen;
- Technologische inzet en innovaties.

Dit heeft geleid tot een eerste selectie van landen: Duitsland (deelstaat, Nedersaksen), Denemarken, België, Frankrijk, Italië, Spanje en het Verenigd Koninkrijk. Op basis van deskresearch is een eerste verkenning gedaan. Op basis van deze verkenning zijn de volgende landen verder verdiept: Frankrijk, België, Italië, Denemarken en Duitsland (deelstaat Nedersaksen). Via de Nederlandse ambassades in de betreffende landen zijn contacten gelegd voor het maken van afspraken van interviews met gesprekspartners. Het verschilde per land hoeveel informatie er kon worden verzameld omdat we sterk afhankelijk waren van de bereidwilligheid van de diensten in de betrokken landen om de onderzoekers van informatie te voorzien. Dit heeft geleid tot een zekere mate van onevenwichtigheid van de verzamelde informatie tussen de verschillende landen. De meeste informatie kon worden verzameld over Italië, België, Duitsland (Nedersaksen), Frankrijk en Denemarken.

Per onderzocht land is steeds (voor zover mogelijk) ingegaan op de volgende kenmerken van het stelsel:

- Rolverdeling en verhouding tussen betrokken organisaties;
- Aanleiding inzet van het stelsel;
- (Dwang)bevoegdheden voor informatieverzameling en dreigingsanalyses;
- Het delen van informatie tussen betrokken partijen;
- Het nemen en uitvoeren van maatregelen;
- Het evalueren/bijstellen van dreigingsanalyses/maatregelen;
- Afbouwen van maatregelen;
- Toezicht op het stelsel.

Bevindingen

Hieronder worden per kenmerk de belangrijkste bevindingen weergegeven.

Rolverdeling en verhouding tussen betrokken organisaties

In alle landen is de politie betrokken bij het stelsel van bewaken en beveiligen, bijvoorbeeld door het aanleveren van informatie voor dreigingsanalyses of het uitvoeren van de beveiliging. Alleen Italië heeft een speciale organisatie (de UCIS) opgericht, specifiek met als doel om het stelsel van bewaken en beveiligen te coördineren. De UCIS heeft verschillende taken, zoals het beoordelen van risicoanalyses, het evalueren van dreigingssituaties en het nemen van maatregelen. Italië maakt geen gebruik van een volledig centraal systeem, want de UCIS wordt nog steeds op lokaal en regionaal niveau ondersteund door politie en prefecten, die verantwoordelijk zijn voor de openbare orde in een bepaald deelgebied van Italië. Het voordeel van een meer gecentraliseerde aanpak, is dat dit in de praktijk heeft geleid tot een betere informatiedeling en coördinatie van het stelsel.

In Frankrijk is er een organisatie (de UCLAT) in het leven geroepen om de samenwerking bij dreigingen vanuit terrorisme te coördineren. In België is ervoor gekozen een organisatie op te

richten die specifiek als taak heeft om dreigingsanalyses voor veiligheidskwesties (waaronder die voor bedreigde personen) te coördineren. België is het enige land waarbij het nationale crisiscentrum een rol heeft in het stelsel, die vergelijkbaar is met de rol van de UCIS in Italië.

Denemarken is het enige land dat volledig centraal georganiseerd is. In Denemarken gaat de veiligheids- en inlichtingendienst hoofdzakelijk over het bewaken en beveiligen van personen. De dienst kan vergeleken worden met een combinatie van de Nederlandse organisaties AIVD, Dienst Koninklijke en Diplomatieke Beveiliging (DKDB) en NCTV. De Deense inlichtingendienst verzamelt de inlichtingen, stelt de analyses op, bepaalt welke maatregelen nodig zijn en voert de fysieke beveiliging vervolgens uit. Om die reden hoeft Denemarken weinig samenwerking tussen partijen te organiseren op dit onderwerp. Dit is opvallend, omdat alle andere landen in dit onderzoek in ieder geval met meerdere partijen samenwerken binnen het stelsel. In Duitsland wordt een onderscheid gemaakt tussen taken op federaal niveau en deelstaatniveau. Op federaal niveau is het Bundeskriminalambt verantwoordelijk voor de beveiliging van een gelimiteerd en specifieke groep personen. De overige taken zijn belegd bij de deelstaten.

Aanleiding voor de inzet van het stelsel

Het proces rondom bewaken en beveiligen kan om verschillende redenen worden ingezet. Uit ons onderzoek is in ieder geval gebleken dat een aangifte in alle landen aanleiding kan zijn om het stelsel in te zetten. Voor België en Italië geldt dat signalen van andere betrokken organisaties het proces ook in gang kunnen zetten. In Italië kunnen er bijvoorbeeld signalen komen vanuit de lokale politie. In België worden signalen van de procureur gebruikt of kan informatie uit overleggen dat het nationaal crisiscentrum voert een aanleiding zijn. Voor België, Italië en Denemarken is het van belang dat een betrokkene aangifte doet, omdat dit de juridische basis vormt voor het inzetten van strafrechtelijke dwangbevoegdheden en om informatie over het dreigingsbeeld te verzamelen. Het valt op dat in België ook signalen uit de media kunnen worden gebruikt.

Dwangbevoegdheden om informatie te verzamelen

Frankrijk heeft een afzonderlijk regime voor het inzetten van dwangbevoegdheden voor het verzamelen van informatie in het kader van de beveiliging van personen. In Frankrijk vallen zowel de inlichtingendiensten als de politie onder de werking van de inlichtingenwet, die hen dwangbevoegdheden geeft om informatie te verzamelen als er sprake is van een terroristische dreiging, zoals het nemen van preventieve maatregelen en beveiligingszones, voor surveillance en monitoring, het onderscheppen van communicatie en het inzetten van noodbevoegdheden. In België geldt voor de inlichtingendiensten dat specifiek in de wet is opgenomen dat zij dwangbevoegdheden kunnen inzetten voor de uitvoering van een beveiligingsopdracht van een persoon. Deze bevoegdheden mogen worden ingezet indien gewone methoden onvoldoende uitkomst bieden en de dwangbevoegdheid passend is gelet op de ernst van de dreiging.

In Italië en België wordt voor de politie volstaan met de ‘klassieke’ bevoegdheden die zij heeft in het kader van het strafrechtelijk onderzoek. Informatie kan daarmee niet op basis van een dwangbevoegdheid worden verzameld in het kader van de veiligheid van een persoon, maar kan alleen ingezet worden in lopende strafrechtelijke onderzoeken. Wanneer betrokkene aangifte doet kan de politie een strafrechtelijk onderzoek starten, waarna deze bevoegdheden kunnen worden ingezet. Hoewel de wetgeving in Denemarken specifiek een koppeling heeft gemaakt met het doen van

onderzoek naar de beveiliging van personen door de inlichtingendienst, geldt dat voor de inzet van dwangbevoegdheden ook sprake moet zijn van een strafrechtelijk onderzoek. Grootste verschil met de andere landen is dat alleen de inlichtingendienst in het kader van de veiligheid van personen deze dwangbevoegdheden uitoefent en niet de politie. In Nedersaksen beschikt Dienst 25 van het Landeskriminalamt over wettelijke bevoegdheden om informatie te vergaren voor het opstellen van risicoanalyses. In geen van de onderzochte landen zijn andere organisaties aangetroffen die over dwangbevoegdheden beschikken, anders dan de politie en inlichtingendiensten.

Informatie delen en verzamelen via andere organisaties

Voor het verzamelen van informatie op basis van open bronnen zijn in de onderzochte landen geen wettelijke bepalingen aangetroffen die dit expliciet reguleren. De grondslagen die hiervoor worden gebruikt zijn algemenere bepalingen op basis waarvan de organisatie de bevoegdheid heeft om informatie te verzamelen. Voor het verzamelen en delen van informatie met/via andere organisaties bestaan in de onderzochte landen verschillende wettelijke bepalingen. Er is geen specifieke wet aangetroffen die enkel betrekking heeft op het delen en verzamelen van informatie in het kader van het bewaken en beveiligen van personen.

Dreigingsanalyses

Voor de dreigingsanalyses geldt dat in alle landen waar deze informatie beschikbaar is, wordt gewerkt met verschillende dreigingsniveaus. Wat betreft terroristische dreigingen is het opvallend dat zowel Italië, België als Frankrijk werken met een specifieke organisatie die het uitvoeren van de dreigingsanalyse coördineert. Bij deze organisatie komt de informatie die is verzameld door verschillende betrokken partijen samen. De precieze rol van die organisatie, en op welke wijze deze informatie wordt gedeeld (zie hiervoor) met deze organisatie verschilt wel per land.

Zo voeren België (OCAD) en Frankrijk (UCLAT) de dreigingsanalyses deels zelf uit op basis van de vertrouwelijke informatie die ze verkrijgen van de politie en inlichtingendiensten, terwijl in Italië deze organisatie (UCIS) slechts de door de politie gemaakte dreigingsanalyse beoordeelt ten behoeve van de uitvoering van de beschermingsmaatregelen. In België maakt het Nationaal Crisiscentrum (NCCN) vervolgens op vergelijkbare wijze een beoordeling van de dreigingsanalyse die (deels) door de OCAD is uitgevoerd en gecoördineerd. Door de scheiding tussen uitvoering en beoordeling van de dreigingsanalyse is het in Italië niet nodig om de onderliggende vertrouwelijke informatie waarop de dreigingsanalyse is gebaseerd schriftelijk te delen

Voor Nedersaksen geldt dat er geen speciale organisatie is opgericht voor coördinatie en uitvoering, maar deze taak is wel belegd bij een specifieke afdeling binnen het Landeskriminalambt en stelt dreigingsanalyses op en neemt maatregelen op basis van politie-informatie. In Denemarken ziet coördinatie er anders uit, doordat het systeem gecentraliseerd is. Gezien zowel het vergaren van de informatie als het maken van de dreigingsanalyse en de beoordeling daarvan ten behoeve van de uitvoering van beschermingsmaatregelen bij de inlichtingendienst is belegd, is het minder nodig voor deze organisatie om samenwerking en het delen van informatie met andere betrokken partijen te organiseren.

Qua uitvoering van de dreigingsanalyse springt Italië eruit, omdat de politie bij terrorisme ook het voortouw heeft om de dreigingsanalyse voor een bepaalde bedreigde persoon op te stellen, terwijl in België, Frankrijk en Denemarken de inlichtingendiensten en/of de coördinerende organisaties hierover

gaan. In Italië levert de inlichtingendienst op dit gebied met name informatie op het niveau van fenomenen, bijvoorbeeld over de aard van een bepaalde terroristische groepering. In het geval van georganiseerde misdaad geldt in België en Italië dat er coördinatie wordt gevoerd door dezelfde organisatie als bij terroristische dreigingen. In Frankrijk ontbreekt deze coördinatie op het gebied van georganiseerde misdaad, en wordt de dreigingsanalyse door de politie uitgevoerd. Denemarken wijkt in het kader van georganiseerde misdaad het meeste af qua werkwijze, omdat de inlichtingendienst wat betreft georganiseerd misdaad ook de dreigingsanalyse uitvoert, en niet de politie.

Maatregelen nemen, evalueren en afbouwen

Uit het onderzoek blijkt dat per land verschilt welke organisatie of persoon bevoegd is om te beslissen of beveiligingsmaatregelen voor bedreigde personen worden ingezet. Dit is een andere vraag dan wie beslist wat de inhoud van deze maatregelen is. Ook verschilt het of deze bevoegdheid is belegd bij één organisatie of meerdere. Voor alle onderzochte landen geldt dat de dreigingsanalyse de basis is voor de te nemen maatregelen. Hoe deze precies doorwerkt in de uiteindelijk te nemen maatregelen verschilt wel per land.

Voor Italië geldt dat zowel de speciaal opgerichte organisatie (de UCIS) als de prefect oordelen of maatregelen ingezet moeten worden. Hoewel er standaardpakketten zijn, verschilt het per dreigingsniveau of maatregelen vooraf vaststaan of dat een afweging nodig is gebaseerd op de specifieke omstandigheden van een situatie. Opvallend aan Italië is dat zij dus niet strikt gehouden zijn aan de dreigingsniveaus en maatregelen, maar dat er ook ruimte is voor maatwerk.

In Frankrijk beslist de minister van Binnenlandse Zaken of maatregelen worden ingezet. Het is niet bekend of Frankrijk gebruikmaakt van standaardpakketten of maatwerk per te beveiligen persoon. De minister oordeelt op basis van dreigingsanalyses en ontvangt advies van een commissie bij het bepalen van de inhoud van de maatregelen.

In België is het Nationaal Crisiscentrum bevoegd om te oordelen of maatregelen worden ingezet. Het NCCN maakt een dreigingsevaluatie op basis van informatie die zij van het OCAD en een afdeling van de politie ontvangt. Op basis van het dreigingsniveau, dat kan variëren van 1 tot 4, wordt bepaald welke maatregelen in een bepaalde situatie passend zijn.

In Denemarken beslist de Politiets Efterretningstjeneste (PET), als verantwoordelijke organisatie binnen het stelsel van bewaken en beveiligen over de inzet van maatregelen.

In alle onderzochte landen vindt evaluatie van de maatregelen en de dreigingsanalyse plaats. Dat gebeurt in ieder geval als er nieuwe informatie beschikbaar is. Hetzelfde geldt voor het afbouwen van maatregelen.

Toezicht

Toezicht op het stelsel van bewaken en beveiligen wordt in de onderzochte landen op verschillende manieren geregeld. Frankrijk heeft een adviesorgaan ingesteld als onafhankelijk toezichthouder. Dit onafhankelijk orgaan kan zowel vooraf, niet-bindend advies uitbrengen over de bevoegdheden van inlichtingendiensten, als achteraf toezicht uitoefenen. Denemarken kent een parlementaire commissie die het doel heeft om toezicht te houden op de Deense inlichtingendiensten. De commissie adviseert de regering mondeling of schriftelijk over de behandelde aangelegenheden. In België zijn twee vaste comités verantwoordelijk voor het toezicht op de deelnemende partijen van het stelsel van bewaken

en beveiligen, ook wat betreft de bescherming van persoonsgegevens. In Duitsland is externe controle geregeld via parlementair toezicht.

De enige instantie die geen officiële toezichthouder heeft in de vorm van commissies of autoriteiten, is Italië. Daar vindt toezicht plaats in de vorm van ministeriële verantwoordelijkheid. De minister van Binnenlandse Zaken is eindverantwoordelijk.

Inspiratie voor het (concept)wetsvoorstel eigenstandige bevoegdheden

Dit onderzoek is uitgevoerd om als inspiratie te kunnen dienen voor het (concept-)wetsvoorstel om eigenstandige bevoegdheden te creëren voor de taken op het gebied van bewaken en beveiligen in Nederland. Omdat de stelsels van bewaken en beveiligen in de onderzochte landen allen functioneren binnen de eigen maatschappelijke en juridische context van die landen, is het niet mogelijk om die stelsels, of zelfs maar specifieke onderdelen daarvan, één op één toe te passen in de Nederlandse situatie. Daarom hebben we een referentiemodel voor een stelsel van bewaken en beveiligen ontwikkeld met ijkpunten die voortkomen uit de bevindingen van het onderzoek. De ijkpunten in het model zijn ingevuld aan de hand van bruikbare voorbeelden van hoe dit in de onderzochte landen is vormgegeven. Het gaat daarbij om de volgende ijkpunten:

- Toegang tot het stelsel is adequaat;
- Coördinatie tussen partijen is adequaat en rolverdeling is helder;
- Er is een heldere juridische basis voor het verzamelen en delen van informatie;
- Er is een heldere juridische basis voor de inzet van dwangbevoegdheden;
- De dreigingsanalyse is adequaat/bruikbaar;
- De evaluatie van maatregelen is effectief;
- Het toezicht is eenduidig en doeltreffend.

Hieronder worden deze ijkpunten van het referentiemodel voor een stelsel van bewaken en beveiligen beschreven en geven we voorbeelden van de wijze waarop een aantal onderzochte landen dit vormgeven en die daarbij als inspiratie kunnen dienen.

De toegang tot het stelsel is adequaat

Bij het vormgeven van de toegang tot het stelsel speelt kort gezegd het dilemma dat het vanuit efficiëntie-oogpunt niet gewenst is dat de drempel te laag is, maar aan de andere kant moeten bedreigde personen wel de weg naar het stelsel weten te vinden. België heeft wat dat betreft een treffende werkwijze. Als iemand aangifte doet wordt deze doorgezet naar het NCCN. Het NCCN beoordeelt de aangifte aan de hand van een dreigingsanalyse en maakt een inschatting van de te nemen beveiligingsmaatregelen. Het NCCN kan ook op basis van andere signalen het beveiligingsproces in gang zetten.

Coördinatie tussen partijen is adequaat en rolverdeling is helder

Voor een adequate en efficiënte coördinatie is het van belang dat het aantal betrokken organisaties beperkt is. Tegelijkertijd kan belangrijke informatie en expertise bij veel verschillende organisaties berusten die relevant kunnen zijn voor de bewaken en beveiligingstaken. In België, Italië en in Duitsland (Nedersaksen) is één orgaan aangewezen dat coördineert. Dat komt in onze ogen toe aan die benodigde mate van doortastendheid, zonder in te hoeven leveren op kennis en expertise.

Er is een heldere juridische basis voor het verzamelen en delen van informatie

Bij informatieverzameling is het enerzijds nodig om voldoende relevante informatie te kunnen verzamelen en delen, anderzijds mag er geen onevenredige inbreuk worden gemaakt op de persoonlijke levenssfeer. In Denemarken heeft de PET de bevoegdheid om zelf alle informatie te verzamelen. Daarnaast mag de PET informatie opvragen van bijvoorbeeld de lokale politie. Dit proces is met passende waarborgen omgeven.

Er is een heldere juridische basis voor de inzet van dwangbevoegdheden

Dwangbevoegdheden kunnen nodig zijn om belangrijke informatie te verzamelen, maar dit moet wel op een manier gebeuren waarbij de ingezette bevoegdheid noodzakelijk en proportioneel is. In Frankrijk zijn de dwangbevoegdheden die mogen worden ingezet duidelijk in de inlichtingenwet geregeld en is bepaald aan welke vereisten geautomatiseerde verwerkingen moeten voldoen en hoe informatie via andere organisaties kan worden verzameld.

De dreigingsanalyse is adequaat/bruikbaar

De te nemen maatregelen moeten in verhouding staan tot het reële dreigingsniveau. Een te veel aan maatregelen is inefficiënt, terwijl te weinig maatregelen veiligheidsrisico's voor betrokkene veroorzaken. Om die reden is een adequate dreigingsanalyse van belang. In Denemarken is die taak toegewezen aan één organisatie die op basis van actuele en brede informatie een analyse uitvoert. Dat leidt tot de hoogste mate van accuraatheid. In België is er een organisatie in het leven geroepen die specifiek gaat over het coördineren van de dreigingsanalyse en het maken van de dreigingsinschatting. Op die manier komt de informatie van de verschillende betrokken partijen met elk hun eigen expertise (georganiseerde misdaad en terrorisme) op één plek bij elkaar.

De evaluatie van maatregelen is effectief

Periodieke evaluaties van de genomen maatregelen zijn van belang om het maatregelenpakket van een bedreigd persoon aan te laten sluiten bij zijn/haar gewijzigde werkelijkheid. Daarbij dient te worden voorkomen dat er te veel of te weinig wordt geëvalueerd. In België en Italië vindt evaluatie van de maatregelen in ieder geval plaats wanneer er nieuwe informatie beschikbaar is die van belang is voor de beveiligingssituatie van een persoon, bijvoorbeeld wanneer iemand wordt gearresteerd. Daarnaast wordt één keer in de drie maanden (België, Italië) of zes maanden (Italië) de casus van een bedreigde persoon besproken in een overleg.

Het toezicht is eenduidig en doeltreffend

Effectief toezicht is cruciaal voor het goed kunnen functioneren van het stelsel. Het dilemma daarbij is dat goed toezicht openheid vergt, maar het is mogelijk dat de aard van bepaalde informatie zich slecht tot dit principe verhoudt. Frankrijk en België hebben dat duidelijk geregeld. In Frankrijk is er een toezichthouder aangewezen die toezicht houdt op het stelsel als geheel. Er is daarnaast een onafhankelijke commissie ingesteld die adviseert over privacyvraagstukken bij de inzet van instrumenten door inlichtingendiensten. Deze commissie kan voorafgaand, niet-bindend advies uitbrengen aan de premier. Ook kan de commissie achteraf toezicht uitoefenen. België heeft ervoor gekozen het toezicht op de deelnemende partijen aan het stelsel van bewaken en beveiligen door twee vaste Comités te laten uitoefenen.

Tot slot

De onderzoekers constateren dat in de onderzochte landen – bezien in de eigen context en geschiedenis van die landen – verschillende keuzes zijn gemaakt bij het inrichten van het stelsel van bewaken en beveiligen. Deze verschillende smaken bieden kansen voor Nederland om daarvan te leren en inspiratie op te doen, door te bekijken of bepaalde elementen zich lenen om toegepast te worden in het Nederlandse stelsel van bewaken en beveiligen. Wij wijzen daarbij in het bijzonder op de manier waarop de coördinerende rol binnen de verschillende stelsels is ingericht, de wijze waarop casusoverleggen worden gehouden en de wijze waarop dwangbevoegdheden bij wet zijn geregeld.

1. Inleiding

1.1 Achtergrond

Nederland is in de afgelopen jaren opgeschud door verschillende (zware) geweldsincidenten gericht tegen personen. In 2018 kwam Reduan B., de broer van kroongetuige Nabil B. in het Marengoproces, om het leven. Hij werd doodgeschoten in zijn eigen bedrijf. Anderhalf jaar later volgde de advocaat van de kroongetuige, Derk Wiersum. Op klaarlichte dag werd hij doodgeschoten op straat. In 2021 werd Peter R. de Vries, de vertrouwenspersoon van de kroongetuige en enkele familieleden, in Amsterdam neergeschoten. Enkele dagen later overleed De Vries aan zijn verwondingen. Hoewel deze personen in beeld waren bij het stelsel Bewaken & Beveiligen (hierna: stelsel B&B) en daarmee door de overheid beschermd werden tegen dreigingen uit de zware, georganiseerde criminaliteit, konden hun levens niet gespaard worden.

Deze aanslagen hebben grote invloed op de democratische rechtsstaat en (het gevoel van) veiligheid en vrijheid. Met het stelsel B&B geeft de overheid uitvoering aan haar zorgplicht om burgers tegen (levens)gevaar te beschermen. Het stelsel staat onder druk en er wordt steeds meer van gevraagd door een stijgende hoeveelheid dreigingen. Uit het dreigingsbeeld van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (hierna: NCTV) uit juni 2025 blijkt dat een aanhoudende dreiging van jihadisme in Nederland bestaat.[1] Ook extremisten en de georganiseerde criminaliteit blijven een gevaar, terwijl zij in snel tempo altijd nieuwe wegen vinden om gevaren voor de samenleving te creëren. Het geweld strekt zich breed uit, tegen onder andere politici, ambtenaren, journalisten, advocaten, (kroon)getuigen en hun familieleden.

Ondanks de bescherming van het stelsel B&B konden de moorden op de broer van de kroongetuige, zijn advocaat en vertrouwenspersoon toch gebeuren. Dit heeft geleid tot onderzoeken en analyses van het stelsel. In 2021 heeft de adviescommissie Toekomstbestendig Stelsel Bewaken en Beveiligen (Commissie-Bos) op verzoek van de minister van Justitie en Veiligheid (hierna: JenV) een analyse gemaakt van de werking van het stelsel en aanbevelingen ontwikkeld om het stelsel te versterken, gelet op de hoeveelheid dreigingen die in een steeds complexer wordende samenleving voorkomen.[2] Meer recent is in 2023 een onderzoeksrapport door de Onderzoeksraad voor Veiligheid (hierna: OVV) opgesteld.[3] De beveiligingssituaties omtrent de drie eerder beschreven personen zijn onderzocht en hebben tot lessen voor de toekomst geleid.

De uitkomsten van deze onderzoeken hebben ertoe geleid dat het stelsel van B&B in 2023 herzien is. Een specifiek belangrijk punt hierbij is de grondslag en daarbij horende knelpunten omtrent het uitwisselen en verzamelen van informatie in beveiligingssituaties. In het hernieuwde stelsel worden onder andere een nieuwe verantwoordelijkheidsverdeling, een beschrijving van informatievergaring- en -deling, en grondslagen om gegevens te verwerken, opgenomen. De politie en de Koninklijke Marechaussee (hierna: KMar) spelen hierin een belangrijke rol.

[1] NCTV 2025. Via https://www.nctv.nl/documenten/2025/06/17/dreigingsbeeld-terrorisme-nederland-juni-2025.
[2] Commissie Bos 2021. Via https://www.nctv.nl/documenten/2021/10/27/rapport-adviescommissie-toekomstbestendig-stelsel-bewaken-en-beveiligen.
[3] Onderzoeksraad voor Veiligheid 2023. Via www.onderzoeksraad.nl.

Het Wetenschappelijk Onderzoek- en Datacentrum (hierna: WODC) heeft gevraagd een rechtsvergelijkend onderzoek uit te voeren naar het bewaken en beveiligen van personen in een aantal Europese landen. Het doel van dit onderzoek is het verschaffen van kennis, inzichten en inspiratie ter voorbereiding van een wetsvoorstel dat bevoegdheden regelt waarmee de politie en KMar informatie kunnen vergaren ten behoeve van het bewaken en beveiligen van personen en voor het maken van dreigingsinschattingen om op basis daarvan een beslissing te kunnen nemen. Ook komen vormen van (externe) controle en toezicht in een aantal Europese landen aan bod.

1.2 Leeswijzer

Het onderzoek is als volgt opgebouwd. Allereerst schetsen wij in hoofdstuk 2 het huidige stelsel bewaken en beveiligen in Nederland, en tegen welke knelpunten dat in de praktijk aanloopt. In hoofdstuk 3 lichten we opdrachtomschrijving en opzet van het rechtsvergelijkend onderzoek toe. In hoofdstuk 4 behandelen we de methodiek. Hoofdstuk 5 staat in het teken van enkele belangrijke artikelen uit het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM), die relevant zijn bij het beveiligen en bewaken van personen. In hoofdstuk 6 gaan wij dieper in op het stelsel van bewaken en beveiligen in zeven geselecteerde landen. In hoofdstuk 7 vergelijken wij de opbrengsten uit de verschillende landen in hoofdstuk 6 met elkaar en lichten wij toe waarin landen overlap vertonen of juist verschillen. We sluiten af in hoofdstuk 8 met inspiratie voor het wetsvoorstel omtrent de bevoegdheden voor bewaken en beveiligen in de vorm van een referentiemodel, en een slotbeschouwing.

2. Bewaken en beveiligen van personen in Nederland

2.1 Inleiding

Voordat wordt ingegaan op de situatie in andere landen, wordt in dit hoofdstuk eerst ingegaan op het Nederlandse stelsel B&B en de knelpunten die worden ervaren. Omdat de opdracht focust op een vergelijking van het stelsel op het punt van de persoonsbeveiliging, beperkt dit hoofdstuk zich ook tot deze taak.

2.2 Het stelsel B&B: verantwoordelijkheden en taken

Het stelsel van bewaken beveiligen in Nederland is ingericht in 2002 naar aanleiding van de aanslag op Pim Fortuyn en heeft als doel het voorkomen van (terroristische) aanslagen op personen, objecten en diensten.[4] Het stelsel is een samenwerkingsverband van verschillende partners, namelijk de NCTV, de politie, het Openbaar Ministerie (hierna: OM), de KMar, de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD) en de burgemeesters. De NCTV heeft een coördinerende taak. Deze instantie brengt beleid en maatregelen samen in het kader van terrorismebestrijding en de bescherming van de nationale veiligheid, met als doel het verhogen van de weerbaarheid tegen dreigingen en risico's, het beschermen van nationale veiligheidsbelangen en het voorkomen van maatschappelijke ontwrichting.[5] Haar taak ziet op het bevorderen van de samenwerking tussen overheidsorganisaties en maatschappelijke organisaties, de samenhang, effectiviteit en evaluatie van beleid, en de informatiedeling tussen overheidsorganisaties voor zover dit noodzakelijk is bij het treffen van maatregelen.[6] De NCTV is verantwoordelijk voor het stelsel van bewaken en beveiligen en draagt hiermee de verantwoordelijkheid voor inrichting, onderhoud en functionering van het stelsel.[7]

Een specifieke wettelijke grondslag voor het samenwerkingsverband is er niet. Aan de minister van JenV, de KMar en de politie zijn bij de wet taken toebedeeld om de rechtsorde te beschermen en te handhaven. De minister van JenV is verantwoordelijk voor het stelsel. De procedures en verantwoordelijkheden zijn vastgelegd in de Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten (voor het laatst gewijzigd in 2023). In de Circulaire wordt ook een aantal uitgangspunten benoemd waarop het stelsel rust.[8] Zo is er volgens de Circulaire sprake van een gelaagde verantwoordelijkheidsverdeling, wat betekent dat personen in beginsel zelf verantwoordelijk zijn voor hun eigen veiligheid. De beveiliging valt onder de verantwoordelijkheid van het decentrale gezag, uitzonderingen daargelaten. Daarnaast worden beveiligingsmaatregelen getroffen op basis van het dreigingsniveau, de dreigingsanalyse en het risico dat een persoon loopt, aldus de circulaire. Daarbij staat veiligheid centraal met oog voor de situatie van de betrokken persoon en worden alleen de maatregelen ingezet die noodzakelijk zijn om de veiligheid van een persoon te kunnen waarborgen. In de uitgangspunten wordt opgemerkt dat volledige veiligheid nooit gegarandeerd kan worden en dat ook na een risico-inschatting nog een restrisico blijft bestaan. Naast veiligheid staat ook maatwerk

[4] Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten, p. 6.
[5] Artikel 2, lid 1 Wet coördinatie terrorismebestrijding en nationale veiligheid.
[6] Artikel 2, lid 2 Wet coördinatie terrorismebestrijding en nationale veiligheid.
[7] https://www.nctv.nl/onderwerpen/b/bewaken-en-beveiligen.
[8] Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten, p. 6-7.

voorop, aldus de circulaire. Het is daarbij van belang dat de te beveiligen persoon meewerkt aan de maatregelen die hem worden opgelegd. Het laatste uitgangspunt is dat het stelsel een lerend systeem dient te zijn dat door de tijd heen aangepast kan worden gelet op ontwikkelingen in de samenleving, en dat wordt ingezet op het continu verbeteren van het stelsel.

Zoals uit de uitgangspunten van het stelsel blijkt, heeft de overheid een zorgplicht om haar burgers te beschermen, maar hebben burgers zelf ook een eigen verantwoordelijkheid om hun veiligheid te garanderen. Naast burgers en de overheid speelt de werkgever een belangrijke rol. Die moet de veiligheid van werknemers zoveel mogelijk proberen te beschermen door maatregelen in en rond de werkplek te nemen. De overheid komt pas in beeld wanneer werkgevers en burgers zelf onvoldoende kunnen doen tegen het dreigingsniveau. Veiligheidsverantwoordelijkheden zijn dus op meerdere plekken belegd.

Daarnaast blijkt uit de uitgangspunten dat de veiligheidszorg voor personen, objecten en diensten in beginsel plaatsvindt onder verantwoordelijkheid van het decentrale gezag (de burgemeester en de hoofdofficier van justitie). De Rijksoverheid heeft een bijzondere verantwoordelijkheid voor een beperkte groep personen, objecten en diensten die door de minister van JenV zijn aangewezen, ook wel het rijksdomein genoemd. De minister van JenV kan objecten en diensten aanwijzen waarvan bewaking of beveiliging door de politie noodzakelijk is in het belang van de veiligheid van de Staat of de betrekkingen van Nederland met andere mogendheden, of met het oog op zwaarwegende belangen van de samenleving.[9] Als zo'n besluit de handhaving van de openbare orde betreft, draagt de burgemeester daarvoor zorg.[10] Als het gaat om de strafrechtelijke handhaving van de rechtsorde is dat de taak van de officier van justitie. De KMar kan assistentie verlenen aan de politie bij onder meer het bewaken en beveiligen van objecten en diensten, onder het lokale gezag. Op decentraal niveau valt de politie onder het gezag van de burgemeester (voor openbare orde) of de officier van justitie (bij strafrechtelijke handhaving).[11] Daarnaast kan de minister van JenV personen aanwijzen die beveiligd dienen te worden.[12]

Naast aangewezen personen kunnen ook andere personen beveiligd worden. In het Nederlandse stelsel van bewaken en beveiligen kan een melding van een concrete dreiging die zich zeer waarschijnlijk of zeker op korte termijn zal voordoen, of een voorstelbare dreiging, op meerdere manier worden gedaan. Dit gebeurt in de praktijk bijvoorbeeld door een aangifte, door aanwijzingen uit de opsporing of intelligence, door de veiligheids- en intelligencediensten of informatie van ketenpartners.[13] Er wordt gewerkt met tabellen om dreigingsniveaus te bepalen. Met behulp van de tabellen kan een inschatting worden gemaakt van de dreiging en welke beveiliging past bij de ernst. Naast een beoordeling van de dreiging worden ook risico's in kaart gebracht en meegenomen bij het oordeel. In Nederland wordt gebruikgemaakt van verschillende informatieproducten om tot een inschatting van dreiging en daarbij horende maatregelen te komen, waaronder een dreigingsinschatting, een dreigingsanalyse en een risicoanalyse.

[9] Artikel 16, eerste lid Politiewet 2012.
[10] Artikel 172 Gemeentewet.
[11] https://www.politie.nl/informatie/kerntaken-politie.html; artikel 124 Wet op de rechterlijke organisatie.
[12] Artikel 42, eerste lid, sub c Politiewet.
[13] Circulaire met betrekking tot de bewaking en beveiliging van personen, objecten en diensten, p. 14.

Casussen worden in het Landelijk Tactisch Overleg besproken (dat zich focust op operationele vraagstukken en casuïstiek om tot landelijke afstemming en besluitvorming te komen) of het Afstemmingsoverleg Bewaken en Beveiligen (in het geval van het rijksdomein).

Een onafhankelijk adviescollege toekomstbestendig stelsel bewaken en beveiligen is ingesteld om advies uit te brengen over het functioneren van het systeem en de doorontwikkeling te bevorderen. Daarnaast monitort de NCTV de kwaliteit van het stelsel en is aan de Inspectie Justitie en Veiligheid een rol toebedeeld om de wettelijke taakuitvoering te toetsen.

2.3 Knelpunten

Zoals eerder beschreven is er geen wettelijke grondslag voor het samenwerkingsverband waarop het stelsel B&B is gebaseerd. De taken die uit het stelsel voortvloeien zijn bij wet toebedeeld aan de minister van JenV en de politie. In de praktijk zijn de taken die uitgevoerd worden door de politie en KMar vastgelegd de Politiewet. De bevoegdheden zijn beperkt tot de algemene taakstelling van de politie, waarbij niet meer dan een 'geringe inbreuk' op de persoonlijke levenssfeer gemaakt mag worden. Door deze beperkingen kan de politie geen diepgaand onderzoek verrichten en kunnen dreigingen blijven bestaan zonder in beeld te komen bij de opsporingsdiensten. Wanneer dus geen strafvorderlijke middelen of bijzondere wetten van toepassing zijn voor de politie om gegevens te verzamelen en onderzoek te doen, kan alleen op basis van de algemene taakstelling informatie worden vergaard. Uit onderzoek blijkt dat deze informatiepositie tot een grote mate van afhankelijkheid leidt om een adequaat dreigings- en risicobeeld op te stellen en gepaste maatregelen te nemen.[14]

Uit onderzoek blijkt ook dat de politie op twee niveaus belemmeringen ondervindt om de juiste informatie te verzamelen en daarmee proactief een dreiging te signaleren en te duiden.[15] Ten eerste wanneer vanuit het perspectief van de bedreiger (een persoon of groepering informatie moet worden verzameld om een concrete dreiging en de modus operandi te detecteren, en ten tweede wanneer vanuit het perspectief van de bedreigde persoon informatie moet worden verzameld om de (potentiële) dreigingen te detecteren en te analyseren.

De algemene bevoegdheid van de politie is volgens de Commissie-Bos in ieder geval onvoldoende om proactief en gericht onderzoek te doen naar dreigingen, aangezien geen gericht en stelselmatig onderzoek mag worden verricht naar personen of groepen op basis van de Politiewet. Het is de vraag in hoeverre de wettelijke bevoegdheden rondom informatieverzameling moeten worden verruimd om wel tot een gedegen onderzoek te kunnen komen.

De OVV concludeert dat politie en OM binnen hun eigen organisaties in 'silo's' werken, wat begrijpelijk is voor de aard van opsporings- en vervolgingstaken.[16] Om passende beveiliging te bieden aan bedreigde personen is het echter van belang dat informatie met verschillende organisatieonderdelen kan worden gedeeld. Alleen op die manier kan een goede risico-inventarisatie gemaakt worden inclusief passende beveiligingsmaatregelen. Het valt in te denken dat minder maatregelen worden ingezet door een gebrek aan informatie. Een persoon kan daardoor meer gevaar lopen, omdat de

[14] Onderzoeksraad voor Veiligheid 2023, p. 110. Via www.onderzoeksraad.nl.
[15] Commissie Bos 2021, p. 52. Via https://www.nctv.nl/documenten/2021/10/27/rapport-adviescommissie-toekomstbestendig-stelsel-bewaken-en-beveiligen.
[16] Onderzoeksraad voor Veiligheid 2023, p.9. Via www.onderzoeksraad.nl.

ingeschatte dreiging niet past bij de realiteit. Tevens kan geen gebruik worden gemaakt van ‘zachte’ informatie, terwijl deze mogelijk zeer interessante en relevante aanknopingspunten bevat. Deze informatie is immers afkomstig van de personen zelf, hun familie, advocaten of vertrouwenspersoon.

3. Opdrachtomschrijving en onderzoeksopzet

3.1 Opdrachtomschrijving

Het doel van het onderzoek is het verschaffen van kennis, inzichten en inspiratie ter voorbereiding van een (concept)wetsvoorstel dat de politie en KMar eigenstandige bevoegdheden geeft voor het verwerven en delen van informatie ten behoeve van het bewaken en beveiligen van personen en voor het maken van dreigingsinschattingen om op basis daarvan een beslissing te kunnen nemen; dat wil zeggen: ook als daarbij een meer dan geringe inbreuk op de persoonlijke levenssfeer wordt gemaakt en het dus een meer stelselmatig optreden betreft.

Daarnaast dient het onderzoek handvatten te geven om een betekenisvolle vorm van (externe) controle en toezicht te creëren/te concretiseren met betrekking tot de uitoefening van bevoegdheden en de handelwijze van de politie inzake B&B.

Het onderzoek dient op beide thema's kennis en inzicht te verschaffen uit buitenlandse rechtsstelsels respectievelijk casussen en zo een inspiratiebron te zijn voor het ontwerpen of wijzigen van Nederlandse wetgeving.

3.2 Onderzoeksopzet

In het onderzoek staan de volgende onderzoeksvragen centraal:

1. Hoe is het bewaken en beveiligen van personen in een aantal EU-landen organisatorisch vormgegeven? Wie zijn hiervoor verantwoordelijk en wie oefenen in de praktijk de bewaking en beveiliging van personen uit?

2. Wat is in de geselecteerde landen het juridisch kader voor de informatieverzameling en informatiedeling met betrekking tot het bewaken en beveiligen van personen? Hoe luiden de online- en offline bevoegdheden om informatie te verzamelen en te delen? Welke wettelijke grondslagen zijn er?

3. Op welke wijze is een externe toetsing op het aanwenden, accorderen en evalueren (controle en toezicht) van de inzet van de bevoegdheden voor het verzamelen en delen van informatie in de geselecteerde landen geregeld?

4. Is in de geselecteerde landen (wetenschappelijk) onderzoek verricht naar de toepassing van de daar geregelde bevoegdheden in de praktijk? Zo ja, in welke mate sluiten de wettelijke bevoegdheden volgens de literatuur aan bij wat in de praktijk nodig is om personen adequaat te bewaken en te beveiligen?

5. Wat is, in aanvulling op de bevindingen van de beantwoording van vraag 4, uit de praktijk van de geselecteerde landen te leren over het verzamelen en delen van informatie in het kader van het bewaken en beveiligen van personen en de bevoegdheden die daarvoor nodig zijn?

6. Welke elementen uit de buitenlandse organisatorische vormgeving en (vigerende of in ontwikkeling zijnde) wet- en regelgeving (volgens de beantwoording van vragen 1 t/m 5)

worden door de onderzoekers aanbevolen als inspiratie voor de inrichting van de Nederlandse systematiek met betrekking tot de bewaking en beveiliging van personen?

3.3 Scope van het onderzoek

In dit onderzoek verkennen we hoe het stelsel van bewaken en beveiligen van personen in een aantal landen werkt. De focus van het onderzoek ligt op personen die bedreigd worden door terrorisme en georganiseerde misdaad, omdat tijdens het onderzoek is gebleken dat deze dreigingen het meest bepalend zijn voor de werking van de verschillende systemen en daarom naar verwachting belangrijke informatie opleveren. De analyse van de landen in dit onderzoek focust op het regime voor bedreigde personen die niet op basis van hun functie standaardbeveiliging ontvangen.

De bescherming van (kroon)getuigen en personen die op basis van hun functie worden beveiligd (VIPS) wordt in dit onderzoek kort behandeld.[17] Doorgaans zijn deze vormen van bescherming via een specifiek stelsel of programma geregeld en valt dit buiten het reguliere stelsel van bewaken en beveiligen. Naar de vorm en effectiviteit van deze regimes is reeds veel onderzoek verricht. Onderhavig onderzoek dient niet specifiek ter inspiratie voor verbeteringen van de Nederlandse stelsels voor de bescherming van VIPS of voor de bescherming van kroongetuigen. Om wel te laten zien dat landen een eigen stelsels voor VIPS en kroongetuigen hebben opgezet en hiervoor maatregelen hebben genomen, lichten wij voor de volledigheid per land kort toe hoe dit eruitziet.

Dreigingen uit de relationele sfeer, femicide of andersoortige dreigingen vallen niet binnen de scope van het onderzoek. Uit de bureaustudie bleek in de landen waar informatie te vinden was over dit type dreiging, het specifieke regime relatief eenvoudig te zijn. Het onderzoek naar de dreiging en de beveiliging ligt met name bij de lokale politie, waardoor het delen van informatie tussen verschillende organisaties binnen het stelsel van bewaken en beveiligen veel minder een thema is bij deze dreigingen. Daarmee draagt een verdere analyse van de wijze waarop dergelijke dreigingen worden opgepakt onvoldoende bij aan het beantwoorden van de vragen die in dit onderzoek centraal staan.

[17] De kring rond (kroon)getuigen, zoals in de paragraaf 1.1 genoemde voorbeelden valt wel onder het ‘gewone’ stelsel B&B zoals dat centraal staat in het onderzoek.

4. Onderzoeksmethoden

4.1 Inleiding

In dit hoofdstuk wordt uitgelegd hoe de onderzoeksvragen worden beantwoord. In eerste instantie was het plan dat het onderzoek uit twee afzonderlijke deelonderzoeken zou bestaan. Het eerste deelonderzoek zou bestaan uit een deskresearch en het tweede deelonderzoek uit een nadere verdieping van enkele landen uit de deskresearch. Beide deelonderzoeken zouden een zelfstandig leesbaar rapport opleveren. Tijdens het onderzoek bleek dit echter niet goed haalbaar, omdat verdiepende interviews cruciaal bleken om de bevindingen van het deskresearch te kunnen verifiëren en waar nodig te corrigeren. Om die reden is er besloten de deelonderzoeken samen te voegen en een overkoepelend rapport op te leveren.

Het onderzoek bestaat uit vier fasen: de selectie van landen, een deskresearch, verdiepende interviews en de vergelijking van de stelsels van de verschillende landen. Hieronder volgt een toelichting op de wijze waarop deze onderzoeksfasen zijn uitgevoerd.

We maken in dit onderzoek gebruik van de functionele methode van rechtsvergelijking. Deze methode gaat er vanuit dat verschillende rechtsstelsels dezelfde maatschappelijke problemen oplossen, hoewel zij dat doen op basis van verschillende rechtssystemen, regels en procedures.[18] Het uitgangspunt is het maatschappelijke probleem dat de landen oplossen. In dit geval de dreigingen tegen personen in het kader van terrorisme en georganiseerde misdaad. Het voordeel van de functionele rechtsvergelijkende methode, in tegenstelling tot de dogmatische methode – waar de vergelijking van vergelijkbare juridische regels of een rechtsgebied centraal staat – is dat de functionele methode erkent dat andere landen een probleem op een hele andere wijze gereguleerd kunnen hebben, bijvoorbeeld in een ander rechtsgebied of rechtsfiguur. Nu juist het doel van de verkennende landenstudie is om inspiratie op te doen en te leren van andere stelsels, is het van belang om te erkennen dat verschillende landen een verschillende aanpak en regulering van het probleem kunnen hanteren. Ten slotte wordt er in de literatuur een onderscheid gemaakt tussen macro-rechtsvergelijking waarin rechtsstelsels in hun geheel worden vergeleken en micro-rechtsvergelijking. Bij micro-rechtsvergelijking worden rechtsstelsels op elementen of onderdelen met elkaar vergeleken. In dit onderzoek passen we een micro-rechtsvergelijking toe. Gelet op de bovengenoemde onderzoeksvragen focussen wij namelijk op een aantal onderdelen binnen het stelsel van bewaken en beveiligen in de betreffende landen.[19]

[18] Zweigert & Kötz 1998.
[19] Gorlé, Bourgeois & Bockert 2007.

4.2 Fase I: selectie van landen

De gehanteerde randvoorwaarden voor de selectie van de landen zijn gebaseerd op de randvoorwaarden die zijn geformuleerd door het WODC.

4.2.1 Randvoorwaarden

Voor het selecteren van de landen gelden de volgende randvoorwaarden.

- Het land ligt binnen de rechtsmacht van het EVRM;
- Er is sprake van een juridisch kader en (een vorm van) gezag en toezicht;
- De bevoegdheid tot bewaken en beveiligen van personen omvat in ieder geval het (online) verzamelen van gegevens;
- De informatie is zonder bovenmatige inspanningen te vinden.

Voor de selectie van landen hebben we een eerste inschatting gemaakt of de informatie zonder bovenmatige inspanningen is te vinden. Deze inschatting hebben we gemaakt op basis van algemene ervaringen en een globale zoekslag naar beschikbare bronnen.

4.2.2 Selectiekenmerken

Naast de randvoorwaarden van het WODC hebben we aanvullende kenmerken/criteria geformuleerd om tot een selectie van landen te komen. Deze staan hieronder weergegeven.

Ordening van de veiligheids- en politiestructuur

Landen met zowel een gecentraliseerde als gedecentraliseerde politie- en veiligheidsorganisatie. Landen met een federale structuur of landen met autonome regio's kunnen interessante contrasten bieden ten opzichte van landen met een meer gecentraliseerd stelsel.

Aard van het rechtsstelsel

Landen met verschillende juridische tradities, zoals het common law-systeem tegenover het continentale rechtsstelsel. Verschillen in rechtsstelsel kunnen van invloed zijn op de inrichting van het stelsel van bewaken en beveiligen en de juridische kaders die van toepassing zijn.

Voorbeeld: Zowel het Verenigd Koninkrijk als Ierland maken gebruik van en common law systeem. Echter, voor Ierland is gebleken dat de informatie niet te verkrijgen was zonder een bovenmatige inspanning te leveren. Daarom is Ierland uiteindelijk afgevallen en is nader onderzoek gedaan naar het Verenigd Koninkrijk.

Culturele en maatschappelijke perceptie van veiligheid

Landen verschillen in culturele en maatschappelijke perceptie van veiligheid. In noordelijke Europese landen ligt de nadruk meer op het waarborgen van burgerrechten en privacy, terwijl in andere landen meer nadruk ligt op veiligheid.

Aanwezigheid internationale instellingen

Landen waar internationale instellingen gehuisvest zijn omdat de aanwezigheid van diplomatieke en internationale organisaties specifieke eisen stelt aan het beveiligingsstelsel.

Historische context en ervaringen met dreigingen

Landen met een lange geschiedenis van interne of externe dreigingen (Spanje en de ETA, Italië en de maffia). Die gebeurtenissen zullen doorgaans een grote invloed hebben (gehad) op de wijze waarop het stelsel van bewaken en beveiligen is ingericht.

Technologische inzet en innovaties

Landen die vooroplopen met de inzet van technologie en innovatie voor beveiligingsdoeleinden.

We hebben landen geselecteerd die zich van elkaar onderscheiden ten aanzien van een bepaald relevant kenmerk. De geselecteerde landen zijn relevant ten aanzien van meerdere kenmerken. Deze methode maakt het eveneens mogelijk om landen uit te sluiten.

Voorbeeld: een land als Zwitserland is relevant ten aanzien van het kenmerk 'aanwezigheid internationale instellingen', maar omdat België ook aan dit kenmerk voldoet en daarnaast relevant is ten aanzien van andere kenmerken (zoals de historische context en ervaringen met dreigingen), kiezen we voor België en niet voor Zwitserland. Een ander element dat daarbij een rol speelt is dat de informatie over het stelsel in Zwitserland niet zonder bovenmatige inspanning te verkrijgen is.

Op basis van de randvoorwaarden en selectiekenmerken zijn we tot de volgende selectie van landen gekomen: het Verenigd Koninkrijk, Ierland, Duitsland (deelstaat, Nedersaksen), Denemarken, België Frankrijk, Italië en Spanje. De onderbouwing hiervoor is weergegeven in onderstaande tabel.

Selectiekenmerk		
Ordening van de veiligheids- en politiestructuur. Landen met een gecentraliseerde politieorganisatie, of juist gedecentraliseerd	*Landen met een federaal/decentraal georganiseerde politie* Duitsland (deelstaten) België (drie gewesten) Spanje (autonome regio's) Verenigd Koninkrijk	*Landen met een gecentraliseerde politie* Frankijk Italië Denemarken
Aard rechtsstelsel	*Common law-stelsel* Het Verenigd Koninkrijk	*Continentaal stelsel* België, Frankrijk, Denemarken, Spanje, Duitsland, Italië
Culturele en maatschappelijke perceptie van veiligheid	*Nadruk op privacy en burgerrechten* Denemarken	*Nadruk op veiligheid* Frankrijk Spanje

		Italië
Aanwezigheid internationale instellingen	België (Brussel)	
Historische context en ervaring met dreigingen	Italië (georganiseerde misdaad/maffia) Spanje (ETA) België (georganiseerde criminaliteit en terrorisme) Verenigd Koninkrijk (terrorisme, moorden op politici)	
Inzet technologie en innovaties	Verenigd Koninkrijk (Closed-Circuit Television)	

De onderzoekers hebben een getrapte wijze van onderzoek gehanteerd. Dit betekent dat is gestart met de bovenstaande selectie van een groep landen die op basis van de randvoorwaarden, kenmerken en criteria geschikt zijn voor het onderzoek, maar waarvan tijdens de deskresearch (zie fase II) nog kon blijken dat een land toch niet geschikt is vanwege een gebrek aan informatie. Vervolgens is voor de geselecteerde landen begonnen met een eerste iteratie van de deskresearch.

Vanuit pragmatische overwegingen is ervoor gekozen om binnen Duitsland onderzoek te doen naar de deelstaat Nedersaksen. Aangezien de verschillende Duitse deelstaten op hun eigen manier invulling hebben gegeven aan het stelsel van bewaken en beveiligen, is ervoor gekozen om één deelstaat uit te lichten. Nedersaksen was bereid om vragen te beantwoorden en aanvullende informatie te verstrekken.

4.3 Fase II: deskresearch

In de tweede fase van het onderzoek is een deskresearch verricht naar de stelsels van bewaken en beveiligen van personen in de geselecteerde landen (België, Denemarken, Duitsland (Nedersaksen), Frankrijk, Italië, Spanje en het Verenigd Koninkrijk). Hiervoor zijn wetteksten, overheidswebsites en wetenschappelijke literatuur geraadpleegd. Van Ierland is zoals eerder benoemd tijdens de deskresearch gebleken dat de informatie niet zonder bovenmatige inspanning is te verkrijgen.

Wat betreft Frankrijk en het Verenigd Konikrijk is alleen deskresearch verricht. Het is voor deze landen niet gelukt om de betrokken organisaties in die landen bereid te vinden om de onderzoekers van aanvullende informatie te voorzien over de werking van het stelsel (zie fase III). Voor deze landen is het belangrijk om op te merken dat de informatie op basis van het open bronnenonderzoek daarom

niet geverifieerd is bij experts, waardoor niet te garanderen is dat alle opgehaalde informatie nog juist en actueel is. Daarnaast geldt dat er voor deze landen minder informatie voorhanden is dan over de landen waar het wel mogelijk was verdiepende gesprekken te voeren met betrokken organisaties.

Daarnaast is tijdens de deskresearch onderzoek gedaan naar de verplichtingen die op staten rusten voor het bewaken en beveiligen van personen op basis van artikel 2 EVRM (recht op leven) en artikel 8 EVRM (recht op de bescherming van de persoonlijke levenssfeer). Dit geeft een beeld van de inspanningen die lidstaten in ieder geval moeten leveren om hun burgers te kunnen beschermen, aan welke randvoorwaarden voldaan moet worden en of de onderzochten landen aan die randvoorwaarden voldoen.

4.4 Fase III: verdiepende interviews

In de derde fase is een verdiepingsslag op de bevindingen uit de deskresearch gemaakt voor de landen België, Denemarken, Duitsland (Nedersaksen), Spanje en Italië. Er zijn in een vroeg stadium van het onderzoek contacten gelegd met liaisons uit de geselecteerde landen. We zijn in contact gekomen met betrokken lokale experts via de ambassades van de betreffende landen. Voor het Verenigd Koninkrijk is het niet gelukt om verdiepende gesprekken te voeren. Hieronder wordt per land uitgelegd welke informatie op welke manier is opgehaald, en welke inspanningen zijn verricht om in contact te treden met lokale experts en liaisons.

België

Voor België heeft een gesprek plaatsgevonden met de Belgische liaisons, het Nationaal Crisiscentrum, het coördinerend orgaan dat dreigingsanalyses opstelt en de centrale directie van operaties inzake gerechtelijke politie. Naar aanleiding van dit gesprek is een aantal aanvullende vragen voorgelegd aan het coördinerend orgaan dreigingsanalyses en het Nationaal Crisiscentrum. Op deze vragen is geen antwoord ontvangen. Wij hebben tevens twee experts gesproken op het gebied van private beveiliging in België. Dankzij deze inzichten was het mogelijk om in kaart te brengen hoe het private systeem is ingericht en op welke gebieden publieke en private beveiliging van elkaar verschillen.

Denemarken

Allereerst heeft een digitaal gesprek plaatsgevonden met twee medewerkers van de Nederlandse ambassade in Kopenhagen. Zij hebben ons geholpen door middel van het in grote lijnen schetsen van het Deense rechtssysteem en van de Deense geheime dienst van de politie (Politiets Efterretningstjeneste, hierna: PET) die onder meer persoonsbeveiliging als taak toegewezen heeft gekregen. Daarnaast hebben we via de Nederlandse ambassade in Kopenhagen contactgegevens gekregen van een medewerker van het Deense ministerie van Justitie, waaraan we onze (schriftelijke) vragen konden stellen.

Duitsland: Nedersaksen

Er zijn contactgegevens aangeleverd van het Nederlandse consulaat in Düsseldorf en een Nederlandse liaisonsofficier van de politie in Düsseldorf. Aan hen zijn verdiepende vragen voorgelegd die doorgestuurd zijn naar Duitse collega's van het Landeskriminalamt Niedersachsen. Zij hebben schriftelijk vragen beantwoord en in een tweede ronde nog aanvullende vragen beantwoord.

Italië

Wat betreft Italië is een gesprek gevoerd met de Italiaanse liaisons van de Nederlandse ambassade in Rome. Om antwoord te kunnen geven op diepgaandere vragen rondom het stelsel van bewaken en beveiligen, hebben de onderzoekers in Rome gesproken met de directeur en de vicepresident van de UCIS, een speciaal opgerichte organisatie die in Italië verantwoordelijk is voor persoonsbeveiliging. Daarnaast was de prefect die portefeuillehouder is van het onderwerp bewaken en beveiligen aanwezig. Beide gesprekken hebben geleid tot waardevolle inzichten over zowel de theorie als de praktijk. De UCIS heeft naast mondelinge ook schriftelijke input aangeleverd. Daarnaast hebben we contact gehad met twee Italiaanse hoogleraren, die schriftelijk vragen over het stelsel hebben beantwoord. Deze academici konden we benaderen omdat deze zich reeds in het netwerk van de onderzoekers bevonden.

Spanje

In het kader van het onderzoek heeft eerst een gesprek plaatsgevonden met de Spaanse liaisons van de Nederlandse ambassade in Madrid. Zij hebben vervolgens een gesprek gevoerd met de Unidad Central de Protección, een onderdeel van de Spaanse nationale politie die onder meer gaat over de bescherming van hooggeplaatste personen en beschermde getuigen. Van het gesprek is een verslag gemaakt door de liaisons en aan de onderzoekers toegestuurd. Het verslag verschafte meer inzicht in het Spaanse stelsel van bewaken en beveiligen, maar niet voldoende om tot verdiepende antwoorden te komen zonder aanvullende gesprekken. Daarnaast is geprobeerd om in contact te komen met een hoogleraar gespecialiseerd in het veiligheidsdomein. Op een daarop gericht verzoek hebben we echter geen reactie ontvangen. Gelet op de beschikbaarheid van bronnen, de bruikbaarheid van de verkregen informatie als ook de inschatting of tot een verdiepingsslag zou kunnen worden gekomen, is besloten om Spanje niet mee te nemen in de verdere verdieping.

Verenigd Koninkrijk

Er een gesprek gevoerd met een liaison van de ambassade van het Verenigd Konikrijk om in contact te komen met Home Office. Deze liaison heeft Home Office benaderd en onze vragen aan deze organisatie voorgelegd. Ook na een verzoek om medewerking van het WODC is het contact noch de medewerking met Home Office tot stand gekomen. Na de komst van een nieuwe liaison heeft deze liaison nogmaals getracht om de vragen beantwoordt te krijgen. Ook deze poging is niet geslaagd.

Op basis van de interviews zijn de opgehaalde inzichten van de deskresearch waar nodig gecorrigeerd en verder aangevuld. Na afronding van fase II en III zijn voor de landen België, Denemarken, Duitsland, Frankrijk, Italië, Spanje en het Verenigd Koninkrijk onderzoeksvragen 1 t/m 5 beantwoord aan de hand van de onderstaande structuur.

- Rolverdeling en verhouding tussen betrokken organisaties
- Aanleiding inzet stelsel
- (Dwang)bevoegdheden voor informatieverzameling en het opstellen van dreigingsanalyses
- Het delen van informatie tussen betrokken partijen
- Het nemen en uitvoeren van maatregelen
- De plichten van de te bewaken persoon
- Het evalueren/bijstellen van dreigingsanalyses/maatregelen
- Het afbouwen van maatregelen

- Toezicht op het stelsel
- VIPS
- (Kroon)getuigen

Zowel tijdens de deskresearch als tijdens de verdiepende gesprekken is niet gebleken dat er wetenschappelijke onderzoeken over dit onderwerp voorhanden zijn in de onderzochte landen. Tijdens het onderzoek is contact gezocht met wetenschappers in de betreffende landen. Dat is gelukt voor Italië, waarbij antwoord is gegeven op schriftelijke vragen. Ook hebben we gesproken met Belgische experts over private beveiliging. Voor Spanje hebben wij wel verzocht om verdiepende vragen te stellen, maar hier is geen reactie op ontvangen. Er is aan het begin van het onderzoek tevens geprobeerd om contact te leggen met Deense wetenschappers. Daar bleek vanuit hun kant onvoldoende tijd voor beschikbaar te zijn. In het contact met deze wetenschappers is niet gebleken dat er wetenschappelijke literatuur beschikbaar was over het onderwerp. Wat betreft de landen waar de wetenschappers ons niet te woord konden staan, is niet bekend in hoeverre er wetenschappelijke literatuur beschikbaar is.

4.5 Fase IV: de vergelijking van de landen

Aan de hand van de opbrengsten over de verschillende onderwerpen per land, is geïnventariseerd welke verschillende modaliteiten er per onderwerp zijn. Op die manier is een beperkt aantal antwoordmodaliteiten per onderwerp onderscheiden. Deze antwoordmodaliteiten zijn omgezet naar een tabel, waarin per land is gescoord welke antwoordmodaliteit per onderwerp van toepassing is. Op deze manier wordt het mogelijk om in een oogopslag de vergelijking tussen de landen te zien voor elk onderwerp. Indien de informatie niet bekend was, is dit ook gescoord.

Vervolgens is, gelet op de beantwoording van onderzoeksvraag 6, beschreven op welke punten landen van elkaar verschillen en is bekeken welke elementen van de verschillende landen eruit springen en interessant zijn voor nadere bestudering en ter inspiratie voor het Nederlands stelsel, bijvoorbeeld omdat een element wezenlijk verschilt van de huidige situatie in Nederland of omdat een kenmerk uniek was voor één land. Ook wanneer een element juist voor veel landen van toepassing is, kan dit interessant zijn. Op deze punten is de vergelijking verder uitgediept.

De vergelijking van de landen is uitgevoerd voor België, Denemarken, Duitsland (Nedersaksen), Italië en Frankrijk. Voor deze landen is voldoende informatie opgehaald om een inhoudelijke vergelijking uit te kunnen voeren. Voor Spanje en het Verenigd Koninkrijk ontbrak te veel informatie, waardoor deze landen niet zijn meegenomen in de vergelijking.

5. Het Europees Verdrag voor de Rechten van de Mens

5.1 Inleiding

Lidstaten van de Europese Unie en het Verenigd Koninkrijk zijn verdragspartij bij het Europees Verdrag voor de Rechten van de Mens (hierna: het EVRM).[20] In dit hoofdstuk wordt nader ingegaan op twee artikelen die van belang zijn bij het beoordelen van de te onderzoeken landen in het licht van het stelsel van bewaken en beveiligen. Het gaat om artikel 2 (bescherming van het recht op leven) en artikel 8 (bescherming van persoonlijke levenssfeer) van het EVRM.

Beide mensenrechten vormen het kader, waarbinnen het stelsel van bewaken en beveiligen dient te worden vormgegeven. Tegelijkertijd kan daarbij een spanningsveld optreden tussen beide artikelen. Enerzijds schept artikel 2 een positieve verplichting voor de landen om noodzakelijke maatregelen te nemen om het leven te beschermen, terwijl artikel 8 EVRM de te treffen maatregelen kan begrenzen doordat de inbreuk op de persoonlijke levenssfeer (van zowel de te beveiligen persoon als de mensen die de dreiging vormen) evenredig moet zijn. Deze twee mensenrechten dienen dan ook gewogen en gebalanceerd te worden. De te onderzoeken landen moeten tenminste voldoen aan beide artikelen om ter inspiratie te kunnen dienen voor de invulling van het stelsel van bewaken en beveiligen in Nederland.

5.2 Artikel 2 EVRM

5.2.1 Inleiding

Hieronder zal eerst worden stilgestaan bij de verhouding tussen artikel 2 van het EVRM en andere verdragen en de verhouding van artikel 2 van het EVRM ten opzichte van het EU-Grondrechtenhandvest. Daarnaast zal worden ingegaan op het toetsingskader aan de hand waarvan het EHRM beoordeelt of een positieve verplichting moet worden aangenomen, wanneer mag worden verwacht dat de Staat feitelijk maatregelen treft om het leven van een burger te beschermen en wat de te nemen maatregelen zijn. Tot slot zal worden ingegaan op het verwerken van persoonsgegevens of onderlinge samenwerking en coördinatie van de betrokken bestuursorganen in het licht van artikel 2 van het EVRM.

5.2.2 Artikel 2 EVRM in relatie tot andere verdragen

De Universele Verklaring van de Rechten van de Mens vormde een basis voor de mensenrechtenverdragen die daarna tot stand zijn gekomen, zoals het EVRM en het Internationaal Verdrag inzake burgerrechten en politieke rechten (hierna: IVBPR).[21] Artikel 3 van de Universele Verklaring van de Rechten van de Mens bepaalt dat iedereen het recht op leven heeft.

[20] Verdrag van 4 november 1950 (*Trb*. 1951, 154).
[21] Verdrag van 19 december 1966 (*Trb.* 1969, 99).

Artikel 2, eerste lid, eerste volzin, van het EVRM, dat zijn evenknie vindt in artikel 6, eerste lid, van het IVBPR, bepaalt dat het recht van eenieder op leven wordt beschermd door de wet.[22] Het Europees Hof voor de Rechten van de Mens (hierna: EHRM) beschouwt de samenloop van de verschillende mensenrechtenverdragen op dat punt van groot belang. Het toont volgens het EHRM aan dat het recht op leven een onvervreemdbaar attribuut van mensen is en de hoogste waarde in de hiërarchie van de mensenrechten vormt.[23]

5.2.3 Verhouding tussen artikel 2 EVRM en het EU-Grondrechtenhandvest

Sinds 1 december 2009 is het EU-Grondrechtenhandvest juridisch bindend voor de instellingen van de EU en voor de lidstaten van de Europese Unie wanneer zij het Europees recht ten uitvoer brengen. Het EU-Grondrechtenhandvest is opgenomen in een verklaring van het Europees Parlement, de Raad en de Europese Commissie, maar heeft dezelfde juridische waarde als de EU-verdragen. De voor dit onderzoek geselecteerde landen die ook lidstaat zijn van de Europese Unie is het EU-grondrechtenhandvest bindend. Uit de preambule van het EU Grondrechtenhandvest volgt dat dit Handvest de rechten bevestigt die (onder meer) voortvloeien uit het EVRM en de rechtspraak van het EHRM.[24]

Het recht op leven is als een zelfstandig recht neergelegd in artikel 2, eerste lid, van het EU-Grondrechtenhandvest en correspondeert met artikel 2 van het EVRM.

5.2.4 Positieve verplichting

Naast een verbod om iemand ongeoorloofd van het leven te beroven, brengt deze bepaling ook de positieve verplichting voor de Staat met zich mee om noodzakelijke maatregelen te nemen om het leven te beschermen van personen die onder zijn jurisdictie vallen.[25]

Vanwege de reikwijdte van het onderzoek concentreert het onderzoek zich op jurisprudentie van het hierna: EHRM over artikel 2 in relatie tot het beschermen van een of meer te identificeren personen die een mogelijk doelwit zijn van dodelijk geweld als gevolg van een criminele handeling van een andere burger.

5.2.5 'Reasonable knowledge and means'-test

Een positieve verplichting wordt aangenomen indien de autoriteiten *kennis* hebben of hadden behoren te hebben van een reëel en onmiddellijk risico voor een identificeerbare persoon of groep personen (het zogenaamde Osman-criterium). Zij dienen dan *maatregelen* te nemen die binnen het

---

[22] Het EHRM heeft het recht op leven omschreven als één van de meest fundamentele bepalingen van het EVRM. Ook het Comité voor de rechten van de mens, dat toeziet op de naleving van de bepalingen uit het IVBPR, heeft het recht op leven betiteld als *the supreme right*. Zie M.C.P. Korten 2015, p. 88. Naast het IVBPR en het EVRM zijn er verdragen die specifiek zien op internationaal beschermde personen, namelijk het Verdrag van Wenen inzake diplomatiek verkeer (Trb. 1962, 101) en het Verdrag inzake de voorkoming en bestraffing van misdrijven tegen internationaal beschermde personen, met inbegrip van diplomaten (Trb. 1981, 69). Nu de VIPS niet centraal staan in dit onderzoek zijn beide verdragen niet verder uitgewerkt.

[23] EHRM 22 maart 2001, 34044/96, 35532/97, 44801/98 (*Streletz, Kessler and Krenz/Germany*), par. 92-94.

[24] De rechtspraak van het EHRM dient in nauwe samenhang te worden bezien met die van het HvJ EU. Dat Hof houdt op grond van artikel 52, derde lid, van het EU-Grondrechtenhandvest rekening met het EVRM en de daarop gebaseerde rechtspraak van het EHRM. Omgekeerd houdt het EHRM in voorkomende gevallen rekening met het EU-recht en de rechtspraak van het HvJ EU daaromtrent. Zie ook Kranenborg & Verhey 2024, p. 34.

[25] EHRM 9 juni 1998, 23413/94 (*L.C.B./VK),* par 36.

bereik van hun macht liggen en die naar redelijke verwachting tot afwending van het risico zullen leiden.[26]

5.2.6 Het Osman-criterium

De verplichting om feitelijke maatregelen te treffen, is voor het eerst uitgewerkt in *Osman t. het Verenigd Koninkrijk*. Het EHRM overweegt in deze zaak dat onder 'certain well-defined circumstances' van de Staat mag worden verwacht dat hij feitelijke maatregelen neemt om het leven van een burger te beschermen tegen de criminele handelingen van een andere burger. Van een schending van artikel 2 EVRM is sprake wanneer:

'the authorities knew or ought to have known at the time of the existence of a real and immediate risk to the life of an identified individual or individuals from the criminal acts of a third party and that they failed to take measures within the scope of their powers which, judged reasonably, might have been expected to avoid that risk.'[27]

Uit het Osman-criterium volgt allereerst dat concrete kennis over de dreigende inbreuk een bepalende rol speelt bij het vaststellen van de verplichting om feitelijke maatregelen te nemen. Het gaat hier om concrete kennis ('knew') over het bestaan van een levensbedreigende situatie. Daarnaast kan het gaan om een geval waarin concrete kennis ontbreekt, maar waarin van de overheid redelijkerwijs wordt verwacht dat zij kennis heeft ('ought to have known'). Er kan alleen een schending worden aangenomen wanneer, gegeven de kennis op het moment van het bestaan van de risico's, niet afgezien had kunnen worden van het nemen van feitelijke maatregelen.[28] Het betreft daarmee een *ex tunc* beoordeling.

Daarnaast dient de situatie een *reëel* en *onmiddellijk* risico te vormen voor het leven (van een of meer specifieke individuen). *Reëel risico* slaat op de mate van waarschijnlijkheid dat de schade zich zal voordoen. *Onmiddellijk* lijkt betrekking te hebben op de mate van afwendbaarheid van het intreden van het risico.[29]

Verder moeten de mogelijke slachtoffers *identificeerbaar* zijn alvorens een positieve verplichting om feitelijke maatregelen te treffen, aangenomen wordt. Er moet dus op de een of andere manier een verband kunnen worden gelegd tussen het levensbedreigende risico en een persoon (of groep personen) die mogelijk slachtoffer kan (of kunnen) worden.[30]

Tot slot mag geen ondraaglijke of buitensporige last – *de bezwaarlijkheid van de te nemen maatregelen* – worden opgelegd aan de autoriteiten, gelet op de moeilijkheden waarmee de politie haar taken in de hedendaagse samenlevingen kan uitoefenen, de onvoorspelbaarheid van menselijk gedrag en operationele keuzes die gemaakt moeten worden in termen van prioriteiten en middelen. Dit betekent dat een vermeende levensbedreiging op zichzelf onvoldoende is om te verplichten tot het nemen van concrete maatregelen.

---

[26] Gerards 2023, p. 183-185; Gijselaar 2021, p. 30.
[27] EHRM, 28 oktober 1998, 23452/94 (*Osman t het Verenigd Koninkrijk),* par 116.
[28] EHRM 15 juni 2021, 62903/15 *(Kurt t. Oostenrijk),* par 160.
[29] Gijselaar 2021, p. 41; EHRM 10 april 2012, 19986/06 *(Ilbeyi Kemaloğlu & Meriye Kemaloğlu t. Turkije),* par 41.
[30] EHRM 28 maart 2000, 22535/93 (*Mahmut Kaya t. Turkije*), par 89.

Bovendien moeten de autoriteiten hierbij ook de andere grondrechten in acht nemen. Die vormen in zekere zin weer een inperking van overheidsmacht.

'In this respect, the Court takes into consideration the need to ensure that the police exercise their powers to control and prevent crime in a manner which fully respects the due process and other guarantees which legitimately place restraints on the scope of their action to investigate crime and bring offenders to justice, including the guarantees contained in Articles 5 and 8 of the Convention.'[31]

5.2.7 Wat zijn zoal de maatregelen volgens het Hof?

Wanneer aan het Osmancriterium is voldaan, dient de Staat maatregelen te nemen. Het EHRM kent de Staat een 'margin of appreciation' toe bij de keuze van de te nemen maatregelen, zeker waar het om 'difficult social and technical spheres' gaat.

Belangrijk vooraf is dat het EHRM heeft bepaald dat als er een verplichting tot handelen ontstaat, dit hoe dan ook een inspanningsverplichting is en geen resultaatsverplichting (obligation of *means*, niet of *result*).

De maatregelen die de Staat treft, moet passen binnen bestaande bevoegdheden. Het is volgens het EHRM nodig dat er een juridisch kader is dat adequaat is. Er moeten dus wel bevoegdheden zijn gecreëerd. '*In other words, the toolbox of legal and operational measures available must give the authorities involved a range of sufficient measures to choose from, which are adequate and proportionate to the level of (lethal) risk that has been assessed. The Court needs to be satisfied, from an overall point of view, that the legal framework was adequate to afford protection against acts of violence by private individuals in any case.'*[32] Ook wordt aangegeven dat onder een adequate preventieve effectieve maatregel valt; *rapid sharing of information among relevant stakeholders.*

De te nemen maatregelen variëren naar context en de aard van de activiteit in kwestie. Waar het om criminele contexten gaat, volgt uit de jurisprudentie van het EHRM dat bijvoorbeeld kan worden gedacht aan allerlei operationele maatregelen, zoals het waarschuwen van burgers en het bewaken en beveiligen van personen, objecten en diensten.[33]

In bepaalde gedefinieerde omstandigheden, is er ook een positieve verplichting voor staten om preventieve maatregelen van praktische aard ('preventive operational measures') te nemen om het individu te beschermen wiens leven wordt bedreigd door de criminele acties van andere burgers[34] Deze beschermingsplicht betreft een inspannings- en geen resultaatsverplichting.[35] Als er dus een positieve verplichting is voor een lidstaat om preventieve maatregelen te nemen en er zijn maatregelen genomen maar de persoon overlijdt alsnog, betekent dit niet dat er dus sprake is van een schending van artikel 2 van het EVRM.

---

[31] EHRM 28 oktober 1998, 23452/94 (*Osman t. het Verenigd Koninkrijk*), par 116.
[32] EHRM 15 juni 2021, 62903/15 *(Kurt t. Oostenrijk),* par 179.
[33] EHRM 13 april 2017, 26562/07 (*Tagayeva e.a. t. Rusland)*, par 489; Gijselaar 2021, p. 43.
[34] EHRM, 28 oktober 1998, 23452/94 (*Osman t het Verenigd Koninkrijk*), par 115; EHRM 28 maart 2000, 22535/93 (*Mahmut Kaya t. Turkije*), par 85; EHRM 28 maart 2000, 22492/93 (*Kılıç t. Turkije*), par 62; EHRM 9 juni 2009, 33401/02 (*Opuz t. Turkije*), par 128.
[35] EHRM 15 juni 2021, 62903/15 *(Kurt t. Oostenrijk*), par 159.

Een andere belangrijke preventieve maatregel is het uitvoeren van een risicobeoordeling (het inschatten van de aard en het niveau van het risico (assessment). De beoordeling of een land zich heeft gehouden aan de eisen van artikel 2 moet gaan over:

- de geschiktheid (adequacy) van de risico-beoordeling door de 'domestic authorities', en
- als er een verplichting was of had moeten worden vastgesteld (duty to act was or ought to have been identified) – de geschiktheid van de preventieve maatregelen.[36]

Als niet kan worden vastgesteld dat de autoriteiten wisten of moesten weten van het bestaan van een risico dat zowel reëel als onmiddellijk was, ontstaat er geen verplichting tot het nemen van preventieve praktische maatregelen. Zie onder meer *Tagiyeva t. Azerbaijan*[37]; er was in deze zaak een fatwa uitgesproken tegen een bekende schrijver enkele jaren voorafgaand aan een verder onverwachte aanslag. Het Hof vond dat niet aannemelijk was dat de autoriteiten de dagen voor de aanslag wisten of moesten weten dat er een reëel en onmiddellijk risico was voor het leven van de schrijver.

5.2.8 De zaak Dink tegen Turkije[38]

In de zaak Dink (een journalist uit Turkije die na zijn detentie voor beledigen van Turkije vanwege zijn standpunt over de Armeense genocide, werd vermoord op straat) werd eerst getoetst of er een reëel en onmiddellijk risico voor het leven van Dink bestond en of de politie op de hoogte was van intense vijandigheid. Het EHRM oordeelde van wel. Het EHRM gebruikt hiervoor de informatie uit het rapport dat in latere strafzaken tegen de moordenaars en medewerkers van de politie is gevoerd. Het EHRM gaat ook in op de specifieke rol van de betrokken instanties: de politie van Trabzon, politie van Istanboel, de gendarmerie van Trabzon en de veiligheidsdiensten van Trabzon en Istanboel. Zij bleken bekend met de waarschijnlijkheid van de moord en zelfs van de identiteit van de mensen die ervan werden verdacht de aanstichters te zijn. Ook waren de daders niet erg discreet geweest bij de voorbereiding.

Het EHRM concludeerde dan ook dat de autoriteiten wisten of hadden moeten weten dat Fırat Dink bijzonder vatbaar was voor een fatale aanval. Bovendien kan dit risico, gegeven de omstandigheden, als reëel en dreigend worden beschouwd.

De vervolgvraag is dan, of de autoriteiten 'alles' hebben gedaan wat redelijkerwijs van hen verwacht kon worden om te voorkomen dat het risico voor Fırat Dink zich zou materialiseren. Het gebruik van het woord 'alles' (*tout* in de officiële tekst) lijkt wel meer te suggereren dan de vraag of de actoren binnen het kader van hun bevoegdheden maatregelen heeft getroffen die vanuit een redelijk standpunt, dit risico ongetwijfeld verkleinen.

Het EHRM kijkt naar drie nationale rechtshandhavingsautoriteiten: de Trabzon-veiligheidsdienst en de Trabzon-gendarmerie, en de Istanboel-veiligheidsdienst. Geen van deze autoriteiten reageerde, gecoördineerd of geïsoleerd, om de moord op Fırat Dink te voorkomen, ook al waren ze op de hoogte van de plannen en de aanstaande aanslag.

---

[36] EHRM 15 juni 2021, 62903/15 *(Kurt t. Oostenrijk),* par 160.
[37] EHRM 7 juli 2022, 72611/14 (*Tagiyeva t. Azerbaijan),* par 60-66.
[38] EHRM 14 september 2010, 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09 (*Dink t. Turkije)*.

Namens Turkije werd aangevoerd dat Dink nooit om directe bescherming van de politie heeft gevraagd. Zijn familie vond dat de politie ambtshalve maatregelen had moeten nemen om de levens van mensen die in direct gevaar verkeren te beschermen. Het EHRM is van oordeel dat Dink weliswaar vijandigheid zal hebben gekend en gevoeld maar dat het voor hem onmogelijk was om informatie te hebben over het feit dat een ultranationalistische groepering in Trabzon een moordaanslag op hem (in Istanboel) voorbereidde. Het was dus de plicht van de nationale autoriteiten, die op de hoogte waren van de planning van de moord in kwestie, om op te treden om het leven van Fırat Dink te beschermen, zonder op zijn verzoek te wachten.

Het Hof concludeert dat de autoriteiten, gezien de bijzondere omstandigheden van de zaak, niet de maatregelen hebben genomen die zij redelijkerwijs hadden kunnen nemen om de verwezenlijking van een reëel en onmiddellijk risico (*risque certain et imminent*) voor het leven van Fırat Dink te voorkomen. Vanuit materieel oogpunt was er dus sprake van een schending van artikel 2 van het Verdrag.

5.2.9 Procedurele component

Artikel 2 kent naast de hiervoor uiteengezette materiële component ook een procedurele component. Dit procedurele deel van dit artikel houdt in dat als er dodelijk geweld is gepleegd, de lidstaat een onderzoek moet doen na afloop (zoals bij de vergiftiging van Navalny)[39], in de vorm van een ‘effective investigation'. Een effectief onderzoek moet geschikt zijn om de omstandigheden te verduidelijken en de verantwoordelijken te identificeren. Het moet onafhankelijk zijn, zowel qua hiërarchie als in de praktijk en moet met redelijke spoed en zorgvuldigheid worden uitgevoerd.[40] In dat kader is het ook noodzakelijk dat er heldere procedures zijn zodat snel kan worden vastgesteld of de procedures wel zijn nageleefd of veranderd moeten worden (en of er dus sprake was van *lack of effective investigation*).

5.3 Artikel 8 EVRM

5.3.1 Inleiding

In deze paragraaf wordt regelgeving besproken die ziet op de bescherming van de persoonlijke levenssfeer, waaronder gegevensbescherming. Toegelicht wordt welke bepalingen uit internationale verdragen en het EU-Grondrechtenhandvest van belang zijn, hoe deze verdragen zich tot elkaar verhouden, wat de voorwaarden zijn waaronder een inbreuk mag worden gemaakt op de daarin vastgelegde fundamentele rechten en hoe deze verdragen doorwerken in de EU-regelgeving en de regelgeving van het Verenigd Koninkrijk.

5.3.2 Artikel 8 EVRM en Conventie 108

Artikel 8 EVRM ziet – evenals artikel 17 van het IVBPR – op de bescherming van de persoonlijke levenssfeer. Dit omvat het recht op de eerbiediging van het privéleven, het familie- en gezinsleven, de woning en correspondentie. Het begrip privéleven moet ruim worden opgevat. Het betreft onder

[39] EHRM 6 juni 2023, 36418/20 (*Navalny t. Rusland no. 3),* par 130.
[40] EHRM 14 september 2010, 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09 (*Dink t. Turkije)*, par. 77.

andere de fysiologische en psychologische integriteit van een individu. Artikel 8 EVRM omvat ook het recht op bescherming van persoonsgegevens.[41]

Artikel 8 luidt als volgt:

1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

In 1981 werd met een verdrag van de Raad van Europa de basis gelegd voor de bescherming van persoonsgegevens: het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Conventie 108).[42] Conventie 108 vormt een uitwerking van het door artikel 8 EVRM beschermde recht op eerbiediging van de persoonlijke levenssfeer met betrekking tot de geautomatiseerde verwerking van persoonsgegevens. Op 10 oktober 2018 te Straatsburg is het Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens tot stand gekomen.[43] Het wijzigingsprotocol voorziet in een groot aantal inhoudelijke en institutionele wijzigingen van het verdrag uit 1981. De wijzigingen die door het wijzigingsprotocol worden aangebracht zijn dermate substantieel dat er materieel gezien een vrijwel geheel nieuw verdrag ontstaat. De inhoudelijke wijzigingen brengen het niveau van de gegevensbescherming dat uit hoofde van Conventie 108 wordt geboden in lijn met het beschermingsniveau dat wordt geboden door het in de afgelopen jaren tot stand gekomen recht van de EU op dit gebied.[44]

5.3.3 Verhouding tussen artikel 8 EVRM en het EU-Grondrechtenhandvest

Het recht op bescherming van persoonsgegevens is als een zelfstandig recht neergelegd in het EU Grondrechtenhandvest. Artikel 7 EU-Grondrechtenhandvest (recht op eerbiediging van het privéleven en van het familie- en gezinsleven) correspondeert met de rechten die artikel 8 EVRM waarborgt en heeft ook dezelfde reikwijdte en inhoud als dat artikel. In artikel 8 EU-Grondrechtenhandvest staat specifiek het recht op bescherming van persoonsgegevens, ook dat artikel is gebaseerd op artikel 8 EVRM.[45]

De Algemene verordening gegevensbescherming (hierna: AVG) en de EU-Richtlijn gegevensbescherming bij rechtshandhaving[46] vormen – wat betreft de bescherming van

---

[41] EHRM 27 juni 2017, 931/13 (*Satakunnan Markkinapörssi Oy en Satamedia Oy t. Finland*), par. 137.
[42] *Trb*. 1988, 7.
[43] *Trb.* 2018, 201; *Trb.* 2023, 54.
[44] *Kamerstukken II* 2023/24, 36455, nr. 3, p. 1-2.
[45] Toelichtingen bij het Handvest van de grondrechten (2007/C 303/(02); Toelichting ad artikel 7, artikel 8 en artikel 52.
[46] 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 (PbEU 2016, L119.

persoonsgegevens – een nadere en gedetailleerde invulling van artikel 8 van het EU-Grondrechtenhandvest en in algemene zin van de fundamentele rechten, zoals neergelegd in artikel 7 van het EU-Grondrechtenhandvest. Die samenhang blijkt ook uit de AVG en de Richtlijn gegevensbescherming bij rechtshandhaving zelf, waarin is bepaald dat deze de grondrechten en fundamentele vrijheden van burgers en met name hun recht op bescherming van persoonsgegevens beschermen.[47] In de lidstaten van de EU zijn de AVG en de EU-Richtlijn gegevensbescherming bij rechtshandhaving is voorzien in nationale uitvoering- respectievelijk implementatiewetgeving (hierna: richtlijn).

Het Verenigd Koninkrijk trad op 31 januari 2020 uit de Europese Unie en is daarom niet langer gebonden aan Europese wet- en regelgeving, zoals de AVG en de EU-Richtlijn gegevensbescherming bij rechtshandhaving. In het Verenigd Koninkrijk geeft de UK General Data Protection Regulation (UK GDPR) en de Data Protection Act 2018 (DPA 2018) een nadere invulling aan artikel 8 EVRM en het wijzigingsprotocol en niet (meer) aan de artikelen 7 en 8 van het EU-Grondrechtenhandvest. De GDPR UK en de DPA 2018 regelt het gegevensbeschermingsrecht in algemene zin en het toezicht daarop. Ook bevat de DPA 2018 een specifieke regeling voor gegevensverwerking door politie en justitie en veiligheidsdiensten. De GDPR UK en de DPA 2018 komt inhoudelijk in belangrijke mate overeen met de AVG en de EU-Richtlijn gegevensbescherming en rechtshandhaving.

5.3.4 Toetsing aan artikel 8 EVRM

Binnen het stelsel van bewaken en beveiligen in de onderzochte landen wordt informatie, waaronder persoonsgegevens, verzameld en gedeeld tussen de verschillende organisaties om dreigingen in beeld te brengen en toereikende maatregelen te kunnen treffen ter bescherming van degene die wordt bedreigd. Het gaat hierbij om persoonsgegevens van zowel de personen die de dreiging vormen, maar ook om de persoonsgegevens van degene die bescherming behoeven.

Het verzamelen en verstrekken (delen) van persoonsgegevens kan leiden tot een inmenging in het privéleven. In deze paragraaf wordt onderzocht wanneer dit het geval is in de zin van artikel 8 EVRM en wanneer deze inmenging gerechtvaardigd is. De toetsing aan artikel 7 EU-Grondrechtenhandvest is gelijk aan artikel 8 EVRM.

5.3.5 Inmenging privéleven?

Artikel 8 EVRM is slechts van toepassing wanneer kan worden vastgesteld dat er sprake is van een inmenging in een privébelang of het privéleven van een individu. Bij het afbakenen van het concept 'privéleven' hanteert het EHRM het criterium van redelijke privacyverwachting, met name met betrekking tot maatregelen in het publieke domein.[48]

Het EHRM heeft meermaals beoordeeld of individuen een redelijke verwachting mogen hebben dat hun privacy wordt gerespecteerd en beschermd. Zelfs in het publieke domein kan een bepaalde mate van interactie tussen een persoon en anderen binnen de reikwijdte van het 'privéleven' vallen. Het

[47] Artikel 1, tweede lid, AVG en artikel 1, tweede lid, onderdeel a, Richtlijn gegevensbescherming bij rechtshandhaving.
[48] EHRM 25 juni 1997, 20605/92 (*Halford t. het Verenigd Koninkrijk),* par. 45; EHRM 5 september 2017, 61496/08 (*Barbulescu t. Roemenië*), par. 73.

EHRM houdt rekening met de mate waarin individuen bewust en opzettelijk deelnemen aan activiteiten die in het openbaar kunnen worden waargenomen en gerapporteerd.[49]

In een online omgeving kan een individu ook een redelijke verwachting van privacybescherming hebben in die zin dat zijn identiteit verborgen blijft.[50] Het feit dat de betreffende persoon vrijwillig en bewust zijn (dynamische) IP-adres bekendmaakt, waardoor hij identificeerbaar wordt voor de website die hij bezoekt, doet in beginsel niet af aan deze verwachting.

Bij gebrek aan jurisprudentie over de redelijke verwachting van privacy in een online omgeving, leiden de onderzoekers uit de jurisprudentie over de privacy verwachting in het (fysieke) publieke domein af dat individuen een verminderde verwachting van privacybescherming hebben wanneer hun informatie beschikbaar is in een online publiek toegankelijke bron. Het EHRM heeft echter geoordeeld dat het enkele feit dat persoonlijke informatie zich in het publieke domein bevindt, niet noodzakelijkerwijs de bescherming van artikel 8 EVRM teniet doet gaan.

Het EHRM houdt rekening met deze redelijke privacyverwachting bij het beoordelen van de ernst van de inmenging. De redelijke privacyverwachting is belangrijk maar niet doorslaggevend bij het bepalen of het privéleven van een individu wordt aangetast.[51] Er moet worden onderzocht of de betreffende handeling daadwerkelijk een inmenging in het recht op eerbiediging van het privéleven vormt. Het privéleven van een individu kan worden aangetast als zijn gedrag systematisch of permanent wordt geregistreerd, Ook wanneer dit plaatsvindt in het publieke domein. Van belang is hierbij of er sprake is van een zodanig indringende vorm van verwerking of gebruik van gegevens dat het privéleven wordt geraakt, bijvoorbeeld in het geval van heimelijke video- en geluidsopnamen van een persoon met het oog op identificatie, of indien video-opnamen uit het publieke domein worden gepubliceerd op een wijze die verder gaat dan het normale of voorzienbare gebruik van dergelijke opnamen.[52]

In het geval van onlinebronnen kan de ernst van de inmenging per geval verschillen, afhankelijk van de intensiteit en aard van het onlineonderzoek. De hoeveelheid verzamelde gegevens over een persoon kan aanzienlijk variëren, maar ook de aard van de gegevens en de wijze waarop deze worden verzameld en de bronnen die daarvoor worden gebruikt, verschillen van geval tot geval.

Wanneer blijkt dat een inmenging in het privéleven plaatsvindt, wordt vervolgens getoetst of deze inmenging gerechtvaardigd is.[53] Deze toets wordt hieronder uitgewerkt. Daarbij wordt uitgegaan van het toetsingskader dat artikel 8, tweede lid, EVRM biedt. Volgens dit artikel dient de inmenging:

- te zijn voorzien bij wet, en;

---

[49] EHRM 17 oktober 2003, 63737/00 (*Perry t. het Verenigd Koninkrijk*), par. 40; EHRM 28 april 2003, 44647/98 (*Peck t. het Verenigd Koninkrijk*) par. 57; EHRM 2 december 2010, 35623/05 (*Uzun t. Duitsland*), par. 43-44.
[50] EHRM 16 juni 2015, 64569/09 (*Delfi AS t. Estland*), par. 147; EHRM 7 maart 2022, 39378/15 (*Standard Verlagsgesellschaft MBH t. Oostenrijk*), par. 76.
[51] EHRM 17 oktober 2003, 63737/00 (*Perry t. het Verenigd Koninkrijk),* par. 37; EHRM 28 februari 2018, 70838/13 (*Antović en Mirković t. Montenegro*), par. 43; EHRM 14 mei 2019, 70573/17 (*Garamukanwa t. het Verenigd Koninkrijk),* par. 22.
[52] EHRM 4 december 2008, 30562/04, 30566/04 (*Marper t. het Verenigd Koninkrijk*), par. 99.
[53] Belangrijk om op te merken is dat in het geval de verwerking van persoonsgegevens geen inbreuk vormt op de persoonlijke levenssfeer van betrokkenen en niet behoeft te worden voldaan aan de voorwaarden voor de inperking van dit recht, bedoeld in artikel 8, tweede lid, EVRM, er wel een rechtsgrondslag als bedoeld in artikel 6 AVG, artikel 8 van de EU-Richtlijn gegevensbescherming en rechtshandhaving respectievelijk artikel 6 van de UK GDPR en artikelen 6, 7 en 35 van de DPA 2018 nodig voor de verwerking van die persoonsgegevens.

- noodzakelijk zijn in een democratische samenleving.

5.3.6 Bij wet voorzien?

Het vereiste dat een inmenging 'bij wet' moet zijn voorzien in de zin van artikel 8, tweede lid, van het EVRM betekent volgens het EHRM dat de aangevochten maatregel een basis in de nationale wetgeving moet hebben en in overeenstemming moet zijn met de vereisten van de rechtsstaat (de 'rule of law'). Dat de maatregel een basis moet hebben in nationale wetgeving is door het EHRM zodanig uitgelegd dat elk algemeen verbindend voorschrift of onder omstandigheden ook rechtersrecht een voldoende rechtsbasis kan zijn voor een inmenging.[54] Deze uitleg van de het EHRM geldt onverminderd de vereisten die voortkomen uit de grondwettelijke orde van verdragspartijen.[55] Voor België en Nederland geldt bijvoorbeeld dat de Grondwet vereist dat een inbreuk op de eerbiediging van de persoonlijke levenssfeer enkel kan plaatsvinden krachtens een wet in formele zin.[56] De Spaanse grondwet schrijft voor dat om een inbreuk op de bescherming van de persoonlijke levenssfeer te mogen maken in specifieke gevallen instemming van een rechter is vereist. Daarnaast wordt bij wet in formele zin het gebruik van geautomatiseerde processen beperkt om de persoonlijke levenssfeer te beschermen en de uitoefening van rechten door de burger te garanderen.[57]

Ingevolge artikel 8 EVRM moet de wettelijke regeling zodanig helder zijn omschreven dat betrokkenen kunnen voorzien onder welke omstandigheden en voorwaarden de autoriteiten een inbreuk kunnen maken op het recht op bescherming van het privéleven.[58]

De eisen die het EHRM stelt aan de grondslag hangen samen met de zwaarte van de inbreuk. In de regel geldt: hoe zwaarder de inbreuk is, hoe preciezer de wettelijke grondslag moet zijn en hoe gedetailleerder moet zijn voorzien in waarborgen, waarbij het geheel van in de wet aanwezige garanties in aanmerking worden genomen.[59]

5.3.7 Noodzakelijk in een democratische samenleving?

De inmenging moet noodzakelijk zijn in een democratische samenleving voor één van de in artikel 8, tweede lid, EVRM opgesomde doelen. Deze doelen betreffen de nationale veiligheid, de openbare veiligheid, het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid en goede zeden of de bescherming van rechten en vrijheden van anderen. Daarbij moet sprake zijn van een dringende maatschappelijke behoefte (pressing social need). De maatregelen moeten proportioneel zijn om het beoogde doel te bereiken. De

[54] EHRM 26 april 1979, 6538/74 (*Sunday Times t. het Verenigd Koninkrijk*), par. 47.
[55] Vergelijk HvJ EU 12 september 2024, ECLI:EU:C:2024:738, par. 68.
[56] Artikel 22 van de Belgische Grondwet en artikel 10, eerste lid, van de Nederlandse Grondwet.
[57] Artikel 18 van de Spaanse Grondwet. De andere onderzochte landen kennen in hun Grondwet dergelijke randvoorwaarden niet om een inbreuk op de persoonlijke levenssfeer te maken.
[58] EHRM 26 april 1979, 6538/74 (*Sunday Times t. het Verenigd Koninkrijk*), par. 49.
[59] EHRM 2 december 2010, 35623/05 (*Uzun t. Duitsland*), par. 66.

rechtvaardigingsgronden aangedragen door de nationale autoriteiten moeten verder relevant en voldoende zijn.[60]

Uitgangspunt is dat de beperking in beginsel niet rechtmatig is als het daarmee beoogde doel ook kan worden bereikt op een wijze die het grondrecht niet of in minder mate beperkt. Laatstgenoemd criterium, ook wel aangeduid als het subsidiariteitsbeginsel, kan worden geacht deel uit te maken van de proportionaliteitstoets. Uit de jurisprudentie van het EHRM blijkt dat veel elementen in de proportionaliteitstoets relevant kunnen zijn. Zo spelen de aard van de gegevens en de reikwijdte van de aangevochten maatregel een rol. Verder kijkt het EHRM, zoals geschreven, naar de waarborgen waarmee de maatregel was omkleed, zoals de aanwezigheid van effectief onafhankelijk toezicht.[61] De informatievergaring binnen het stelsel van bewaken en beveiligen raakt aan het doel van de bescherming van de nationale en openbare veiligheid en aan de bescherming van de rechten en vrijheden van anderen en voorziet in een dringende maatschappelijke behoefte.

5.4 Weging artikelen 2 en 8 EVRM

Hoe verhouden de artikelen 2 en 8 van het EVRM zich tot elkaar? Dient de overheid voorrang te geven aan een van deze grondrechten?

Het recht op bescherming van de persoonlijke levenssfeer moet ten dienste staan van de mens. Het recht op bescherming van de persoonlijke levenssfeer heeft geen absolute gelding, maar moet worden beschouwd in relatie tot de functie ervan in de samenleving en moet conform het evenredigheidsbeginsel tegen andere grondrechten, zoals het recht op leven, worden afgewogen.[62]

De weging van deze grondrechten vindt op meerdere niveaus plaats. Allereerst vindt deze weging plaats op het niveau van de wet, waarbij moet worden beoordeeld of de beperking van fundamentele rechten van burgers voldoet aan eisen van noodzakelijkheid, proportionaliteit en subsidiariteit.

Daarnaast vindt de weging van grondrechten plaats in het individuele geval. In dat licht is het van belang om te onderkennen dat op de overheid een inspanningsverplichting en geen resultaatsverplichting rust om te voorkomen dat er een schending ontstaat van de artikelen 2 en 8 van het EVRM. De overheid behoeft deze mensenrechten dan ook niet ten koste van alles te beschermen. In het licht van de jurisprudentie van het EHRM is het verdedigbaar dat individuele zelfbeschikking een groot goed is dat gerespecteerd dient te worden.[63] Wanneer iemand de aangeboden bescherming weigert, dient de overheid dit te respecteren. Dat neemt niet weg dat het niet uit te sluiten is dat de overheid niettemin – met inachtneming van de houding van de in gevaar verkerende persoon – dient te bezien of er redelijkerwijs beschermingsalternatieven bestaan om te voorkomen dat de bestaande

[60] EHRM 22 oktober 1981, 7525/76 (*Dudgeon t. Verenigd Koninkrijk*), par. 51; EHRM 22 juni 2023, 10794/12 (*Giuliano Germano t. Italië*), par. 96; EHRM 20 juni 2023, 36705/16 (*Margari t. Griekenland*), par. 53.
De grondbeginselen van deze toets vinden hun oorsprong in oudere rechtspraak. Zie EHRM 7 december 1976, 5493/72 (*Handyside t. Verenigd Koninkrijk*) par. 48 en EHRM 26 april 1979, 6538/74 (*Sunday Times t. Verenigd Koninkrijk),* par. 59. Deze zijn daarna leidraad gebleven en toegepast in vele arresten.
[61] Kranenborg & Verhey 2024, p. 48-54.
[62] In lijn met overweging 4 van de AVG zij het dat deze overweging zich beperkt tot de bescherming van persoonsgegevens dat onderdeel is van het recht op bescherming van de persoonlijke levenssfeer.
[63] Zie EHRM 29 juli 2007*,* 2346/02 (*Pretty t. Verenigd Koninkrijk*), par. 61; EHRM 24 september 2007, 5410/03 (*Tysiac t. Polen),* par. 105-108.

dreiging tot uitvoering komt. De feiten en omstandigheden van het geval, waaronder de houding van de te beschermen persoon, zullen daarbij een belangrijke rol spelen.[64]

[64] Korten 2015, p. 98.

6. Analyse van de onderzochte landen

In dit hoofdstuk komt de landenanalyse van België, Denemarken, Duitsland (Nedersaksen), Frankrijk, Italië, Spanje en het Verenigd Koninkrijk aan bod. Op basis van deskresearch en interviews met betrokken organisaties in deze landen, wordt geschetst hoe het stelsel van bewaken en beveiligen in deze landen die vallen onder de rechtsmacht van het EVRM eruitziet. In dit hoofdstuk wordt antwoord gegeven op onderzoeksvragen één tot en met drie en vijf. Deze vragen hebben betrekking op de organisatorische vormgeving van bewaken en beveiligen in andere landen, hoe het juridisch kader voor en de praktische werking van informatieverzameling en -deling eruitzien en hoe toezicht wordt uitgeoefend.

Per land volgt een inleiding om te schetsen welke rol bewaken en beveiligen speelt in een bepaald land. Vervolgens bespreken we welke organisaties betrokken zijn bij persoonsbeveiliging, wat hun onderlinge rolverdeling is en hoe zij zich tot elkaar verhouden. Hierna bespreken we wanneer het stelsel ingezet kan worden, hoe informatie wordt verzameld en gedeeld tussen betrokken organisaties en hoe dreigingsanalyses worden opgesteld. Ook komt aan bod hoe het nemen, uitvoeren, evalueren en afbouwen van maatregelen is vormgegeven. Ten slotte wordt uiteengezet hoe het toezicht per land is geregeld.

Voor elk land wordt na de inleiding de situatie weergegeven voor personen die bedreigd worden vanuit terrorisme en georganiseerde misdaad. Voor zogenoemde VIPS geldt een ander regime. Dit wordt aan het eind van elke landenparagraaf in een aparte subparagraaf beschreven. Daarnaast wordt kort ingegaan op het regime voor de bescherming van (kroon)getuigen.

6.1 België

6.1.1 Inleiding

Een belangrijk thema op de veiligheidsagenda van België is het bestrijden van terrorisme en radicalisering.[65] In de jaren 80 werd België een aantal keer opgeschrikt door aanslagen tegen Israëlitische en joodse doelwitten. Ook kampte België in die jaren met een ernstige terreurgolf veroorzaakt door de CCC en de Bende van Nijvel. Om dergelijke dreigingen het hoofd te bieden, werd op 17 september 1984[66] de Antiterroristische Gemengde Groep opgericht. De Antiterroristische Gemengde Groep was de voorloper van het Coördinatieorgaan voor de dreigingsanalyse (OCAD), dat in 2006 het stokje overnam. De doelstelling van deze groep is behouden gebleven. Het OCAD maakt analyses en evaluaties op basis van de informatie en inlichtingen die het van de partners krijgt. De laatste vijftien jaren heeft het land te maken gehad met verschillende terroristische aanslagen en terroristische dreigingen. De meest ingrijpende terroristische aanslagen waren die van zelfmoordterroristen bij de luchtenhaven en het metrostation in Brussel in 2016. Een recenter incident in 2023 betrof een aanvaller die twee Zweedse burgers doodde in Brussel. Naar aanleiding van dit incident heeft België aanpassingen doorgevoerd om dreigingen beter het hoofd te kunnen bieden,

[65] https://www.belgium.be/nl/justitie/veiligheid/terrorisme.
[66] Pas bij koninklijk besluit van 17 oktober 1991 werd de organisatie en de werking van de Antiterroristische Gemengde Groep daadwerkelijk in regelgeving neergelegd. Ook werd met dat koninklijk besluit de groep overgeheveld van het ministerie van Justitie naar het ministerie van Binnenlandse Zaken.

onder andere door de federale politie te versterken met extra capaciteit en de informatiestromen tussen immigratiediensten, de politie en justitie te versterken.[67]

Brussel is het centrum van de Europese Unie, wat betekent dat er veel internationale overleggen, evenementen en conferenties plaatsvinden. Zo vond er in oktober 2023 een EU-top plaats, een week na de aanslag op de twee Zweedse burgers, waardoor België genoodzaakt door het verhoogde risico extra voorzorgsmaatregelen nam.[68]

6.1.2 Rolverdeling en verhouding tussen betrokken organisaties

In België zijn het Coördinatieorgaan voor de Dreigingsanalyse, het Nationaal Crisiscentrum, de directie van de operaties inzake gerechtelijke politie, de federale politie, de Algemene Dienst Inlichting en Veiligheid[69], en de lokale politie (bestaande uit 185 politiezones) betrokken bij het bewaken en beveiligen van personen.[70]

Het Coördinatieorgaan voor de Dreigingsanalyse (hierna: OCAD) is een orgaan dat is belast met het vaststellen en de evaluatie van de dreigingsniveaus voor heel België of voor specifieke locaties, evenementen of personen.[71] Dit orgaan speelt een centrale rol in het nationale beveiligingsstelsel. Als coördinerende instantie zorgt het OCAD voor de verspreiding van relevante dreigingsinformatie aan alle betrokken partijen, waaronder lokale en federale politiediensten, andere betrokken overheidsinstanties, waaronder het Nationaal Crisiscentrum, en privé-beveiligingsbedrijven. Dit zorgt ervoor dat alle partijen geïnformeerd blijven over actuele en potentiële dreigingen. Het OCAD is geen inlichtingen- of politiedienst. Dit orgaan staat onder het gemeenschappelijke gezag van de minister van Justitie en de minister van Binnenlandse Zaken. Beide ministers zijn in beginsel gezamenlijk belast met de organisatie en het algemeen bestuur van het OCAD.[72] Het OCAD is een autonome organisatie binnen de Staat. Binnen het OCAD is het Departement Punctuele Analyse belast met de taak tot het opstellen van punctuele dreigingsevaluaties. Deze dreigingsevaluaties hebben onder meer betrekking op de extremistische of terroristische dreiging ten aanzien van personen in België. Dit departement bestaat uit personeelsleden gedetacheerd uit de ondersteunende diensten van het OCAD. Zij vervullen de rol van verbindingsofficier tussen het OCAD en hun dienst van oorsprong.[73]

---

[67] https://www.politico.eu/article/belgium-announce-new-security-measures-brussels-attack/.
[68] https://www.euronews.com/2023/10/25/brussels-on-security-alert-ahead-of-eu-leaders-summit.
[69] De Wet op het Politieambt in België biedt een algemeen kader voor de bevoegdheden van de politiediensten. De wet bevat verder geen specifieke taken of bevoegdheden voor de politiediensten die zien op de bewaking en beveiliging van personen. Echter deze wetgeving biedt wel een grondslag om informatie, waaronder persoonsgegevens, te kunnen verwerken en te verstrekken.
[70] De Wet op het Politieambt in België biedt een algemeen kader voor de bevoegdheden van de politiediensten. De wet bevat verder geen specifieke taken of bevoegdheden voor de politiediensten die zien op de bewaking en beveiliging van personen. Echter deze wetgeving biedt wel een grondslag om informatie, waaronder persoonsgegevens, te kunnen verwerken en te verstrekken. Zie voor de opbouw van de politie in België de Wet tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus van 7 december 1998.
[71] De Wet betreffende de analyse van de dreiging en het onderliggende Koninklijk besluit reguleert reguleren de structuur en de taken van het Coördinatieorgaan voor de Dreigingsanalyse (het OCAD). Deze wet legt de basis voor hoe dreigingsanalyses worden uitgevoerd, welke instanties betrokken zijn, en hoe informatie gedeeld wordt tussen verschillende veiligheidsdiensten.
[72] Artikel 4 van de Wet van 10 juli 2006 betreffende de analyse van de dreiging in samenhang bezien met de artikelen 2 en 3 van het Besluit tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging.
[73] OCAD 2023. Via https://ocad.belgium.be/wp-content/uploads/2024/07/Jaarverslag_2023.pdf.

Het Nationaal Crisiscentrum (hierna: NCCN)[74] valt onder het ministerie van Binnenlandse Zaken en coördineert de bescherming van bedreigde personen[75], maar is geen inlichtingen- of veiligheidsdienst. Het NCCN heeft geen zelfstandige informatiepositie en is afhankelijk van informatie van andere diensten om zijn coördinatietaak te kunnen uitoefenen. Het NCCN treft in elk dossier en voor elke betrokken persoon specifieke maatregelen. De lokale politiediensten voeren de maatregelen uit.

Binnen de Federale Politie – als onderdeel van de Algemene directie van de gerechtelijke politie – is de Directie van de operaties inzake gerechtelijke politie (hierna: DJO) verantwoordelijk voor het beheer en coördinatie van operaties. Bij het uitvoeren van haar opdrachten zet de DJO een breed scala van specifieke deskundigheden in ter ondersteuning van de politie waaronder het NCCN.[76]

De Algemene Dienst Inlichting en Veiligheid (hierna: ADIV) richt zich primair op de nationale veiligheid, defensie en militaire belangen van België en heeft geen rechtstreekse rol bij de beveiliging van specifieke personen. Toch kan haar werk ook raakvlakken hebben met de beveiliging van individuen.[77] De vergaarde inlichtingen en dreigingsanalyses van de ADIV kunnen een ondersteunende rol bieden in het beveiligen van belangrijke personen in de context van de nationale defensie en veiligheid.

De lokale politie is verantwoordelijk voor de bescherming aan de te beschermen personen binnen hun regio, bijvoorbeeld door middel van surveillance en patrouilles. Ook in geval van incidenten, is de lokale politie vaak de aangewezene om de eerste vormen van beveiliging te bieden voordat gespecialiseerde eenheden worden ingezet.

Het AIK (Arrondissementeel Informatie Kruispunt) heeft tot taak om ‘de juiste (verrijkte) informatie, op het juiste moment, op de juiste wijze, aan de juiste “belanghebbenden” (lokale en federale politiediensten, overheden van bestuurlijke en gerechtelijke politie) te bezorgen’. Het AIK verrijkt informatie door exploitatie en exploratie van de beschikbare informatie. Dit omvat bijvoorbeeld het detecteren van linken tussen gerechtelijke feiten op basis van tijd, plaats, modus operandi. Dit gebeurt binnen en over de arrondissementsgrenzen heen. Ook de fenomeenopvolging (van bijvoorbeeld inbraken) o.a. met het oog op patroondetectie. Deze ‘intelligence’ biedt een meerwaarde, bijvoorbeeld voor de lokale politie, om meer actiegericht te kunnen werken.[78]

Private beveiliging

Ook vanuit de private sector kan persoonsbeveiliging verzocht worden. De keuze voor private persoonsbeveiliging in plaats van publieke persoonsbeveiliging kan meerdere redenen hebben, bijvoorbeeld omdat er te weinig capaciteit beschikbaar is bij de publieke sector, of omdat personen zelf kiezen voor een meer preventieve vorm van beveiliging (bijvoorbeeld wanneer er nog geen

[74] Opgericht bij Koninklijk besluit van 18 april 1988 tot oprichting van het Coördinatie en Crisiscentrum. Bij Ministerieel besluit van 22 april 2003 tot bepaling van de administratieve behandelingsprocedure van de aangelegenheden bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus is het Coördinatie en Crisiscentrum overgegaan in de Algemene Directie Crisiscentrum. Hetgeen later is gewijzigd in het NCCN.
[75] Artikel 2, derde lid, van het Ministerieel besluit van 22 april 2003 tot bepaling van de administratieve behandelingsprocedure van de aangelegenheden bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus.
[76] https://www.politie.be/5998/nl/over-ons/federale-gerechtelijke-politie/centrale-directie-van-operaties-inzake-gerechtelijke.
[77] https://vsse.be/nl/dreigingen.
[78] https://www.jobpol.be/nl/federale-politie/coordinatie-en-steundirectie-halle-vilvoorde#about-us.

concrete dreiging is, maar deze mogelijk wel gaat komen). Private bewaking en beveiliging is strikt wettelijk geregeld via de Wet tot regeling van de private en bijzondere veiligheid en Wet tot regeling van de private opsporing. In de wet staat beschreven binnen welke domeinen welke beveiligingsactiviteiten uitgevoerd mogen worden. Op deze activiteiten wordt intensief toezicht uitgeoefend door diensten van het ministerie van Binnenlandse Zaken. Voor hun informatie zijn de beveiligingsorganisaties afhankelijk van hun opdrachtgever; er is op het gebied van persoonsbescherming geen sprake van een publiek-private samenwerking.

6.1.3 Aanleiding inzet van het stelsel

In België kunnen er meerdere aanleidingen zijn om het stelsel in te zetten. Het startpunt ligt in het merendeel van de gevallen bij de lokale politie waar de betrokkene aangifte doet van een bedreiging aan het adres van de betrokkene. Het doen van aangifte vormt de juridische basis voor de politie om bevoegdheden uit het Wetboek van Strafvordering te kunnen aanwenden. Nadat de aangifte is gedaan informeert de lokale politie het NCCN en stuurt met de aangifte de relevante informatie naar het NCCN. Denk hierbij aan contactgegevens van de betrokkene, het proces-verbaal, en andere informatie die nodig is om beveiliging te kunnen bieden.

Signalen van een dreiging komen niet alleen bij het NCCN door middel van een aangifte. Ook kan het NCCN van een dreiging op de hoogte raken door bijvoorbeeld signalen uit de pers, van de procureur of uit het overleg tussen het NCCN en de kabinetten van ministers. Wanneer de dreiging het NCCN niet bereikt door middel van een aangifte is het van belang dat in de andere gevallen alsnog aangifte wordt gedaan. Aangifte is namelijk noodzakelijk om bevoegdheden uit het Wetboek van Strafvordering te kunnen inzetten en om informatie te verkrijgen over een actueel beeld van het dreigingsniveau. Na de aangifte wordt onderzoek gedaan door de gerechtelijke politie die onderdeel uitmaakt van de Federale Politie.

6.1.4 (Dwang)bevoegdheden voor informatieverzameling en dreigingsanalyses

Nadat het signaal van een bedreigd persoon bij het NCCN is binnengekomen, vraagt het NCCN – afhankelijk van het type dreiging – het OCAD en/of de DJO om het maken van een dreigingsanalyse en het vaststellen van een dreigingsniveau. Het OCAD beoordeelt de dreiging vanuit het oogpunt van terrorisme en extremisme. De DJO kijkt naar de dreiging vanuit het perspectief van de georganiseerde criminaliteit.

Dreigingen vanuit terrorisme

Het OCAD analyseert alle relevante informatie en inlichtingen over terrorisme, extremisme en problematische radicalisering. Het OCAD heeft geen eigen dwangbevoegdheden om zelf informatie en inlichtingen te verzamelen. Voor het opstellen van een dreigingsanalyse baseert het OCAD zich op voor de zaak relevante informatie die reeds door de ondersteunende diensten (veiligheidsdiensten, zoals de ADIV, politiediensten, gevangenissen) is bewerkt, geanalyseerd en beoordeeld op basis van hun (dwang)bevoegdheden. De veiligheidsdiensten mogen in het kader van de veiligheid van de staat (waaronder dreigingen vanuit terrorisme en georganiseerde misdaad) dwangbevoegdheden inzetten (zoals onderscheppen (tele)communicatie, observatie in publiek toegankelijke plekken) indien gewone onderzoeksmethoden zoals openbaar bronnenonderzoek ontoereikend zijn. Hiervoor is toestemming nodig van de bestuurlijke commissie die toezicht houdt op de inzet van deze methoden. Ten slotte kent deze wet nog een categorie ‘uitzonderlijke methoden’ (zoals afluisteren, observatie in niet publiek

toegankelijke plaatsen en het binnendringen van een ICT-systeem). Deze kunnen enkel worden ingezet na machtiging van het diensthoofd na eensluidend advies van de hierboven genoemde commissie. De methoden moeten in functie van de graad van de ernst van de potentiële bedreiging worden gekozen.[79] Deze diensten zijn verplicht om desgevraagd reeds verzamelde informatie aan het OCAD mede te delen.[80] Er bestaat een afwijkend regime – de embargoprocedure – voor inlichtingen van gerechtelijke aard en inlichtingen die worden meegedeeld aan het OCAD door ondersteunende diensten afkomstig van een soortgelijke buitenlandse dienst. Voor deze inlichtingen wordt, onder bepaalde voorwaarden, voorzien dat zij op zodanige wijze kunnen worden meegedeeld dat ongecontroleerde verspreiding van deze soms gevoelige informatie wordt vermeden. Het NCCN ontvangt enkel de noodzakelijke informatie om maatregelen te kunnen opleggen die de bescherming van de bedreigde persoon zullen verzekeren.[81]

Het dreigingsniveau kan variëren van laag (niveau 1) tot zeer ernstig (niveau 4), afhankelijk van de actuele ernst en de dreiging die daarvan uitgaat. Deze dreigingsniveaus helpen het NCCN bij het bepalen van de aard en omvang van de beveiligingsmaatregelen die moeten worden toegepast.

Dreigingen vanuit georganiseerde misdaad

De DJO voert de analyse uit vanuit het perspectief van de georganiseerde criminaliteit en maakt daarbij net als het OCAD gebruik van de reeds verzamelde en geanalyseerde informatie afkomstig van de politie dat is verkregen door middel van onderzoeks- en dwangbevoegdheden in het kader van strafrechtelijk onderzoek.[82] De DJO heeft dus geen eigen dwangbevoegdheden die het specifiek kan inzetten in het kader van de beveiliging van personen. De DJO stelt het hierboven beschreven dreigingsniveau vast en deelt de noodzakelijke informatie met NCCN.

Indien er sprake is van een gemengde dreiging, onderzoeken het OCAD en de DJO de dreiging vanuit hun eigen, gespecialiseerde invalshoeken. Het is mogelijk dat het OCAD en de DJO vanuit hun eigen expertise tot andere conclusies komen over welk dreigingsniveau geldt. Het NCCN neemt in dat geval het hoogste dreigingsniveau tot uitgangspunt.

6.1.5 Het delen van informatie tussen betrokken partijen

Artikel 13bis van de Wet op het Politieambt bevat de verplichting voor de gerechtelijke overheden, de ambtenaren en agenten van de openbare diensten om aan de Minister van Binnenlandse Zaken alle nuttige inlichtingen mede te delen die ze bezitten en die betrekking hebben op de bescherming van het leven of de fysieke integriteit van de te beschermen personen. Daarnaast bevat artikel 44 van deze wet regels over de verwerking van persoonsgegevens ter uitvoering van deze wet. Zo bevat artikel 44/5, eerste lid, onderdeel 4, een grondslag voor de verwerking van persoonsgegevens van subjecten

[79] Artikelen 12-18 (specifiek artikel 18 en 43) Wet betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten; artikel 46b Wetboek van Strafvordering. Artikel 24 benadrukt dat officieren die belast zijn met de uitvoering van de bescherming van personen ook over deze bevoegdheden beschikken.
[80] Artikel 6 in samenhang bezien met artikel 14 van de Wet van 10 juli 2006 betreffende de analyse van de dreiging en Wetsontwerp betreffende de analyse van de dreiging, *Kamer* 2005/06, doc. 51 nr. 2032/001, p. 16. Dat de partnerdiensten wettelijk verplicht zijn om alle relevante inlichtingen en informatie aan het OCAD te bezorgen, betreft een belangrijk verschil met de Antiterroristisch Gemengde Groep.
[81] Artikel 15 van het Koninklijk besluit van 20 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging.
[82] Artikel 46bis Wetboek van Strafvordering.

die schade kunnen toebrengen aan te beschermen personen. In artikel 44/11/8bis is geregeld dat OCAD de informatie van de politiediensten kan ontvangen. De artikelen 13bis en 44/11/8bis zorgen als spiegelbepalingen ervoor dat aan de verplichting om informatie (desgevraagd) te leveren (zoals bepaald in de artikelen 6 en 14 van de Wet betreffende analyse en dreigingen) voldaan kan worden.

De Wet van 30 juli 2018 is zowel de uitvoeringswet voor de AVG als ook de implementatiewet voor de Richtlijn (EU) 2016/680.[83] Titel 1 van de wet is gericht op de AVG en Titel 2 implementeert de richtlijn. Er is ook een derde Titel, 'De bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door andere overheden dan die bedoeld in titels 1 en 2'. Ondertitel 4 van Titel 3 van deze wet gaat over de verwerking van persoonsgegevens door het OCAD.[84] Deze ondertitel is van toepassing op elke verwerking door het OCAD en zijn verwerkers voor de uitvoering van opdrachten in het kader van de wet van 10 juli 2006 betreffende de analyse van de dreiging (artikel 139).[85]

Het OCAD mag, voor zover hier van belang alleen persoonsgegevens verwerken als (artikel 140), de verwerking noodzakelijk is voor de vervulling van een taak van openbaar belang.

Persoonsgegevens moeten behoorlijk en rechtmatig verwerkt worden voor duidelijke en gerechtvaardigde doelen, en mogen daarom niet verder verwerkt worden voor onverenigbare doelen, moeten toereikend zijn voor het doel en moeten nauwkeurig zijn.[86] Het OCAD mag bijzondere persoonsgegevens verwerken voor zover dit noodzakelijk is voor de uitvoering van zijn opdrachten.[87] Persoonsgegevens worden niet langer bewaard dan noodzakelijk, hiervoor zijn regels opgesteld in artikel 9 van de wet van 10 juli 2006. In die wet als ook in de Uitvoeringswet zijn regels gesteld over de te treffen technische en organisatorische beveiligingsmaatregelen. Ook voorziet de uitvoeringswet in een wijze waarop wordt omgegaan met onder meer de rechten van betrokkenen, inbreuken in verband met persoonsgegevens en de doorgifte naar derde landen en internationale organisaties.

Voor het NCCN lijken – los van de meer in zijn algemeenheid gestelde regels in de Uitvoeringswet AVG en Richtlijn 2016/680 – geen specifieke regels te gelden voor de verwerking van persoonsgegevens. Zo heeft het NCCN ook geen eigen wettelijke taken of specifieke grondslag om zelfstandig gegevens te mogen verzamelen. Wie van mening is dat het NCCN zijn rechten op het gebied van gegevensbescherming niet respecteert, kan zich wenden tot de Belgische Gegevensbeschermingsautoriteit.[88] Wel voorziet de wetgeving aangaande de andere betrokken organisaties, zoals het OCAD en de Wet op het Politieambt om informatie aan het NCCN te verstrekken, voor zover noodzakelijk voor de uitvoering van zijn taak.

Op het NCCN rust de plicht om de dreiging te beheersen en maatregelen in te zetten. Wanneer bescherming aan een persoon wordt gegeven, vindt er op initiatief van het NCCN een casusoverleg

---

[83] Richtlijn (EU) 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.
[84] Sinds 2024 is de gemeenschappelijke gegevensbank "Terrorisme, Extremisme, Radicaliseringsproces" aan deze Ondertitel toegevoegd.
[85] Artikel 139 van de Uitvoeringswet AVG en Richtlijn (EU) 2016/680.
[86] Artikel 141 van de Uitvoeringswet AVG en Richtlijn (EU) 2016/680.
[87] Artikel 142 van de Uitvoeringswet AVG en Richtlijn (EU) 2016/680.
[88] https://crisiscentrum.be/nl/privacyverklaring.

plaats. Het NCCN roept alle diensten bijeen om helderheid te krijgen. Er is geen verplichting voor die diensten om daaraan deel te nemen. Wat er besproken wordt met de diensten is heel breed, bijvoorbeeld ook de mentale gezondheid van de persoon die wordt bedreigd. Tijdens dit overleg is er eveneens oog voor de familie van de bedreigde persoon.[89] Het NCCN kan niet rechtstreeks opdracht geven om ten behoeve van het overleg informatie te verkrijgen. De informatie wordt opgehaald door een verzoek daartoe bij het OCAD en de DJO. Dit betreft reeds bekende informatie. Wanneer aangifte is gedaan, kan ook informatie worden gekregen over de in het geding zijnde dreiging.

6.1.6 Het nemen en uitvoeren van maatregelen

Om de bedreigde personen te beschermen, bepaalt het NCCN beschermingsmaatregelen op basis van een dreigingsevaluatie. In de eerste plaats wordt getracht om door middel van ingrepen in de leefwereld het risico maximaal te vermijden (dat kan bijvoorbeeld door bepaalde plaatsen te mijden). Daarna worden bijkomende beschermingsmaatregelen vastgesteld. De maatregelen kunnen al dan niet zichtbaar, preventief of reactief zijn.

Er kunnen op basis van het dreigingsniveau verschillende maatregelen worden genomen. De meest lichte vorm is een contactpersoon bij de lokale politie die spelregels met de betrokkene doorneemt (wat moet je doen wanneer je een verdachte auto ziet, wanneer bel je het noodnummer, etc.).

In zeer uitzonderlijke gevallen kunnen de maatregelen verdergaand zijn, zoals close protection (24/7 persoonsbescherming) of zelfs het direct onderbrengen in een safe house. Dit soort maatregelen heeft echter een bijzonder grote impact op de persoon in kwestie en wordt dus enkel genomen in geval van een grote en zeer concrete dreiging.[90]

Bij niveau 4 bepaalt de Federale politie of de noodzaak bestaat om de beschermingscommissie te verwittigen. Dit is een zeer uitzonderlijke situatie. De maatregelen zijn in dat geval tijdelijke of permanente identiteitswijziging of het onderbrengen in een safehouse voor meer dan 45 dagen.

De uitvoering vindt plaats door de lokale politie. De lokale politie staat namelijk het dichtst bij de burger; de Federale Politie is daar verder van verwijderd.

Er is geen informatie bekend over de plichten waar een te bewaken persoon zich aan moet houden.

6.1.7 Het evalueren/bijstellen van dreigingsanalyses/maatregelen

Het NCCN houdt elke drie maanden overleg over een lopende casus, tenzij eerder overleg noodzakelijk is. Een nieuwe gebeurtenis, bijvoorbeeld een arrestatie, kan een reden zijn om eerder in overleg te gaan. In dit casusoverleg is er ook oog voor bijvoorbeeld de mentale gezondheid van de betrokkene en voor de familie van de bedreigde persoon.

[89] De werkwijze van het NCCN is vastgelegd in een omzetbrief (circulaire) vanwege het vertrouwelijke karakter daarvan hebben de onderzoekers geen kennis kunnen nemen van die omzetbrief.
[90] https://crisiscentrum.be/nl/newsroom/2024-kregen-101-personen-bescherming-na-bedreigingen-de-uitoefening-van-hun-functie.

Er bestaat een vertrouwelijke omzendbrief die het Belgische stelsel van bewaken en beveiligen operationaliseert. Deze omzendbrief bevat bindende richtlijnen voor betrokken diensten. De brief beschrijft procedures rond dreigingsinschatting, informatiedeling, besluitvorming en inzet van beschermingsmaatregelen bij bedreigde personen, met aandacht voor samenwerking, proportionaliteit en evaluatie van maatregelen. De omzendbrief kon in het kader van deze internationale verkenning niet gedeeld worden door de Belgische autoriteiten.[91]

6.1.8 Afbouwen van maatregelen

In de overleggen van het NCCN worden lopende casussen besproken. Hierin wordt per casus besproken of de getroffen beveiligingsmaatregelen nog volstaan of dat de maatregelen kunnen worden afgebouwd.

6.1.9 Toezicht op het stelsel

In België wordt het toezicht uitgeoefend door twee vaste Comités. Het toezicht op de politiediensten wordt uitgevoerd door het Vast Comité van Toezicht op de politiediensten (Vast Comité P). Het toezicht op het OCAD wordt uitgevoerd door het Vast Comité van Toezicht op de inlichtingendiensten (hierna: Vast Comité I) en het Vast Comité P.[92] Krachtens artikel 1 van de wet tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse heeft het toezicht van het Vast Comité I en het Vast Comité P in het bijzonder betrekking op de bescherming van de rechten die de Grondwet en de wet aan de personen waarborgen. In artikel 161 van de Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens is bepaald dat het Vast Comité I, als onafhankelijke publieke autoriteit, en het Vast Comité van Toezicht op de politiediensten, worden aangewezen als gegevensbeschermingsautoriteiten belast met de controle van de verwerking van persoonsgegevens door het OCAD en zijn verwerkers volgens de nadere regels vastgelegd in de wet van 18 juli 1991. Daarmee vormen deze twee comités de exclusieve onafhankelijke toezichthouder en niet het COC en de gegevensbeschermingsautoriteit.

6.1.10 VIPS

In België worden de leden van het koningshuis standaard beveiligd. Er is echter geen wetgeving in België die bepaalde functies of personen beschrijft die automatisch beveiliging krijgen binnen het stelsel van bewaken en beveiligen.[93] In hoeverre er een regime voor VIPS is vastgesteld in interne, niet-openbare overheidsdocumenten konden deze documenten in dit onderzoek niet worden achterhaald. Voor zover bekend geldt er voor overige VIP-functies geen standaard beveiliging, dit wordt per casus bepaald door het NCCN.[94]

[91] Deze informatie blijkt uit het gesprek met de Belgische autoriteiten.
[92] https://www.comiteri.be/index.php/nl/; https://comitep.be/index.html?lang=nl.
[93] https://www.monarchie.be/en/monarchy/royal-household/security-detail.
[94] https://www.vrt.be/vrtnws/nl/2024/07/15/politici-beveiliging-trump-belgie/.

De leden van het Koninklijk huis worden standaard beveiligd, ongeacht of er een dreiging bestaat of niet. Een permanent Veiligheidsdetachement van de federale politie beveiligt de leden van het Koninklijk huis. Deze staat onder bevel van de hoofdcommissaris.[95] De minister van Binnenlandse Zaken is verantwoordelijk voor de veiligheid van leden van het Koninklijk huis.

6.1.11 (Kroon)getuigen

De bescherming van getuigen is sinds 2002 wettelijk geregeld.[96] Artikel 104 van het Wetboek van strafvordering bepaalt, in samenhang met artikel 102, dat beschermingsmaatregelen kunnen worden getroffen ten behoeve van getuigen die gevaar lopen als gevolg van afgelegde of af te leggen verklaringen. Voor zover gezinsleden en andere bloedverwanten ook gevaar lopen, komen zij ook in aanmerking voor bescherming.

Artikel 105, eerste lid, van het Wetboek van strafvordering bepaalt dat een verzoek tot het toekennen van beschermingsmaatregelen kan worden gedaan door het Openbaar Ministerie of de rechter-commissaris. Een bestuurlijk orgaan van de Federale Overheidsdienst Justitie – de Getuigenbeschermingscommissie – beslist op dat verzoek. Die commissie valt onder de (politieke) verantwoordelijkheid van de minister van Justitie. De Getuigenbeschermingscommissie beslist ook over het wijzigen of intrekken van maatregelen.[97]

Intrekking gebeurt volgens artikel 108, vierde lid van het Wetboek van strafvordering als betrokkene geen gevaar meer loopt. Volgens hetzelfde artikel vervallen de beschermingsmaatregelen voor een bedreigde getuige zodra deze officieel verdacht of vervolgd wordt voor de feiten waarover hij heeft getuigd. Dat gaat dus nadrukkelijk over de procedure waarin dan wordt getuigd. Kroongetuigen worden meestal wel verdacht van strafbare feiten, maar dan in een andere procedure.[98] De vraag is wel in hoeverre dat strookt met de verplichting van Staten tot bescherming van de veiligheid van haar burgers.

6.2 Denemarken

6.2.1 Inleiding

Het stelsel van bewaken en beveiligen in Denemarken onderscheidt zich van andere landen, doordat er voor een andere inrichting van het stelsel is gekozen. Een van de belangrijkste verschillen is dat er in Denemarken sprake is van een relatief gecentraliseerd systeem, met een geïntegreerde aanpak waarbij de Deense Veiligheidsdienst zowel gaat over inlichtingenverzameling, het opstellen van dreigingsanalyse, het nemen van de beveiligingsmaatregelen als de fysieke beveiliging. Ook in Denemarken is een van de belangrijke veiligheidsthema's op het gebied van het bewaken en beveiligen van personen het tegengaan van terrorisme, en is er sprake van een verhoogde waakzaamheid gelet op mogelijke dreigingen van terrorisme.

---

[95] https://www.monarchie.be/nl/monarchie/werking/veiligheidsdetachement.
[96] Wet houdende een regeling voor de bescherming van bedreigde getuigen en andere bepalingen, 7 juli 2002. Deze wet wijzigt bepalingen in het (Belgische) Wetboek van strafvordering.
[97] Tegen beslissingen staan geen rechtsmiddelen open, zo volgt uit te artikelen 105, tiende lid en art. 109, zevende lid van het Wetboek van strafrecht.
[98] Vergelijk het met de situatie van Nabil B.; hij werd zelf verdacht van overvallen en getuigde in de liquidatiezaak Marengo.

Zo werd de cartoonist Kurt Westergaard sinds 2005 beveiligd vanwege zware bedreigingen uit radicaalislamitische hoek, naar aanleiding van een cartoon over de profeet Mohammed. Verder voerden de Deense inlichtingendienst en de politie in 2023 nog enkele arrestaties uit in verband met het plannen van terroristische activiteiten.[99] Het grootste gedeelte van de activiteiten van de Deense inlichtingendienst is gefocust op het tegengaan van terrorisme, maar er bestaan ook dreigingen uit rechts- en links-extremistische hoek.[100] Vorig jaar bleef het dreigingsniveau op level 4 (uit 5), maar uit de nationale risico-inventarisatie blijkt dat de daadwerkelijke dreiging wel degelijk is toegenomen.[101]

6.2.2 Rolverdeling en verhouding tussen betrokken organisaties

In Denemarken zijn de volgende organisaties in hoofdzaak betrokken bij het bewaken en beveiligen van personen: de Politiets Efterretningstjeneste (hierna: PET, specifiek de Persoonlijke Beschermingseenheid), de nationale politie (Rigspolitiet) en de lokale politie. Ook is de militaire inlichtingendienst Forsvarets Efterretningstjeneste (hierna: FE) betrokken.

De PET valt onder het Deense Ministerie van Justitie.[102] De dienst kan gezien worden als een combinatie van de Nederlandse organisaties AIVD, DKDB en NCTV.[103] Defensie ondersteunt de Nationale Politie waar mogelijk bij het vergroten van de nationale veiligheid.[104] In Denemarken is de FE zoals gezegd verantwoordelijk voor militaire inlichtingen.[105] De FE maakt jaarlijks inlichtingenrisico-inventarisaties en valt onder het ministerie van Defensie.[106] Denemarken kent geen militaire politie zoals we in Nederland de Koninklijke Marechaussee hebben.[107] Naast de PET en de FE bestaat er een nationaal Center for Cybersikkerhed (Centrum voor Cybersecurity).[108]

De taak van de Deense politie-inlichtingendienst is volgens artikel 1, eerste lid, van de PET-wet als volgt.[109] PET onderzoekt en gaat misdrijven tegen de onafhankelijkheid en veiligheid van de staat, alsmede misdrijven tegen de staatsgrondwet en de hoogste staatsautoriteiten, te onderzoeken en tegen met betrekking tot de preventie en het onderzoek van strafbare feiten uit hoofdstuk 12 (Misdrijven tegen de soevereiniteit en veiligheid van de staat) en hoofdstuk 13 (Misdrijven tegen de staatsgrondwet en de hoogste staatsautoriteiten, etc.) van het Deense Wetboek van strafrecht. Dit is de belangrijkste taak van de PET. Die taak wordt ook bedoeld waar in het hiernavolgende wordt gesproken over ‘de taak’ (van de PET). Artikel 1, tweede lid, van de PET-wet bepaalt dat de PET in het kader van die taak dreigingsanalyses opstelt.

De PET is primair verantwoordelijk voor het bewaken en beveiligen van de Koninklijke familie, regeringsfunctionarissen, andere hoogwaardigheidsbeklederes en voor individuen die onder

---

[99] https://www.gbnews.com/news/world/denmark-terror-attack-arrests-copenhagen-danish-security-and-intelligence-service.
[100] https://pet.dk/en/threats-to-denmark/terrorism-and-extremism.
[101] https://www.reuters.com/world/europe/terrorism-threat-against-denmark-has-increased-security-service-says-2024-03-21/.
[102] https://pet.dk/en/about-pet/organization.
[103] Bakker & Vos 2023, p 9.
[104] Forsvarsministeriet, Danish Defense Agreement 2018-2023.
[105] https://www.fe-ddis.dk/en/.
[106] https://www.fe-ddis.dk/en/produkter/Risk_assessment/.
[107] Bakker & Vos 2023, p 10.
[108] https://www.cfcs.dk/da/.
[109] Voluit: Lovbekendtgørelse 2017-03-07 nr. 231 om Politiets Efterretningstjeneste (PET). Vertaling: Wet van 7 maart 2017 nr. 231 betreffende de Politie Inlichtingendienst (PET).

aanzienlijke dreiging staan. De PET werd opgericht in 1951, maar is in de laatste twee decennia aanzienlijk belangrijker geworden.[110] Alle persoonlijke bewakingsopdrachten worden uitgevoerd door deze dienst.[111] De te bewaken personen worden zowel internationaal als nationaal het hele jaar door gevolgd.[112] Daarnaast gaat de PET over de dreigings- en risicoanalyses voor de bewaking en beveiliging van deze personen en beslist de PET ook over de te nemen maatregelen. Binnen de PET is een opsporingsteam werkzaam voor het onderdeel bewaken en beveiligen.[113] Hoewel de verschillende verantwoordelijkheden allen bij de PET zijn ondergebracht, werken de onderdelen wel semi-onafhankelijk van elkaar.

Ten slotte is de nationale politie betrokken bij het reageren op specifieke dreigingen tegen personen. Dit kan inhouden dat ze snel reageren op incidenten of dreigingen in de buurt van beschermde personen en samenwerken met de veiligheidsdiensten om een gecoördineerde reactie te waarborgen.

6.2.3 Aanleiding inzet van het stelsel

Over de aanleiding van de inzet van het stelsel in Denemarken is geen (publiek toegankelijke) informatie bekend. Zoals in de volgende paragraaf zal worden beschreven, heeft de PET een (vrij algemene) bevoegdheid die – kort gezegd – strekt tot voorkoming van misdaden tegen onder meer de staatsveiligheid. De bevoegdheden tot informatieverzameling die die taak met zich meebrengt, resulteert in het feit dat de PET een goede informatiepositie heeft. Het ligt voor de hand dat die informatiepositie maakt dat de PET informatiegestuurd bepaalt of er al dan geen aanleiding bestaat voor de inzet van het stelsel.

6.2.4 (Dwang)bevoegdheden voor informatieverzameling en dreigingsanalyses

De PET-wet vormt het wettelijk kader voor het bestaan en handelen van de PET.[114] De regels met betrekking tot het verzamelen, opvragen, verwijderen, openbaar maken en andere vormen van verwerking van informatie door PET zijn geregeld in hoofdstuk 2 (verstrekking van informatie), hoofdstuk 5 (interne verwerking van informatie), hoofdstuk 6 (openbaarmaking van informatie) en hoofdstuk 7 (wettige politieke activiteiten). De Deense regering werkt aan een nieuwe PET-wet.

Op basis van artikel 1, zesde lid, van de PET-wet heeft de PET de taak om personen te beschermen. De bevoegdheid van de PET om informatie te verkrijgen is geregeld in de artikelen 3 en 4 van de PET-wet. Uit artikel 3 van de wet volgt dat de PET informatie mag verzamelen en verkrijgen die van belang kan zijn voor de activiteiten van de dienst. Volgens de toelichting bij de PET-wet betekent het criterium “van belang kunnen zijn” dat het verzamelen en verkrijgen van informatie door de dienst alleen moet voldoen aan een algemene relevantievoorwaarde, wat betekent dat niet bij voorbaat kan worden uitgesloten dat de informatie relevant is voor de dienst.[115]

Zoals hiervoor beschreven behoort het opstellen van een dreigingsanalyse tot de kerntaak van de PET (artikel 1, tweede lid, van de PET-wet). Daarvoor verzamelt de PET informatie, zowel openbaar als niet

---

[110] De Graaff 2018, p. 95.
[111] https://pet.dk/en/our-tasks/security#:~:text=PET%20is%20responsible%20for%20all,and%20individuals%20under%20particular%20threat.
[112] https://pet.dk/en/our-tasks/security/the-personal-protection-unit.
[113] Bakker & Vos 2023.
[114] Officieel: Lovbekendtgørelse 2017-03-07 nr. 231 om Politiets Efterretningstjeneste (PET).
[115] Pagina 57 van de toelichting bij de PET-wet.

openbaar. Het “verzamelen” van informatie verwijst naar het verstrekken van informatie die direct beschikbaar is, bijvoorbeeld in de vorm van krantenartikelen, brochures en informatie uit elektronische media. Het “verkrijgen” van informatie verwijst naar het verstrekken van informatie die niet direct beschikbaar is, maar kan worden verkregen door contact op te nemen met een derde partij, bijvoorbeeld een overheidsinstantie, vereniging, organisatie, bedrijf of particulier.

Artikel 5 bepaalt dat de PET ook zelf onderzoeken kan instellen tegen natuurlijke personen en rechtspersonen indien de onderzoeken van belang kunnen zijn voor de uitvoering van de taken van de dienst. Artikel 6 van de wet bepaalt dat voor het onderzoek en de toepassing van dwangbevoegdheden (zoals observaties, huiszoekingen, inzage in telecommunicatie, etc.) het Wetboek van Strafvordering van toepassing is.[116] Voor de inzet van dit type bevoegdheden moet daarom sprake zijn van een lopend strafrechtelijk onderzoek en is in de regel toestemming vereist van bijvoorbeeld de rechter.[117]

6.2.5 Het delen van informatie tussen betrokken organisaties

De relevante wetgeving omtrent het delen van gegevens door de PET is gestructureerd in hoofdstuk 5 en verder van de PET-wet. Deze bepalingen geven de PET de bevoegdheid om gegevens door te geven aan de FE, mits dit relevant is voor de uitvoering van haar taken. Voor het verstrekken van persoonsgegevens aan andere Deense bestuursorganen, private partijen, buitenlandse autoriteiten en internationale organisaties gelden de artikelen 6a en 7 van de PET-wet. Wanneer het gaat om privéaangelegenheden, is aanvullend artikel 8, tweede lid, van de Deense wet op gegevensbescherming van toepassing.[118] Voor rechtspersonen zijn de bepalingen in artikel 6a, leden 1-5 en 7 en artikel 8 van de PET-wet relevant. Gegevensdeling mag uitsluitend plaatsvinden na een concrete beoordeling en wanneer dit als verantwoord kan worden aangemerkt, waarmee de wetgeving waarborgen biedt voor zorgvuldigheid en proportionaliteit.

De PET gebruikt kennis van hun inlichtingenwerk om kritieke en kwetsbare doelwitten te identificeren in relatie tot terrorisme en andere bedreigingen. Deze analyses helpen bij het plannen en uitvoeren van beveiligingsopdrachten en zijn essentieel voor het handhaven van de nationale veiligheid en de bescherming van belangrijke personen. De analyses worden gedeeld met de Deense politiedistricten om hen in staat te stellen de nodige beschermingsmaatregelen en tegenmaatregelen te initiëren met betrekking tot specifieke evenementen of bedreigingen. Deze samenwerkingsbenadering zorgt ervoor dat er een gecoördineerde respons is tussen nationale en lokale beveiligingsinspanningen. De directeur-generaal van PET rapporteert direct aan de Minister van Justitie.[119]

In Denemarken wordt gewerkt met meerdere dreigingsniveaus die vergelijkbaar zijn met het systeem in Nederland.[120] Beide landen werken richting risicobeperking in plaats van risico-uitsluiting. Er is amper sprake van publiek-private samenwerking op het thema bewaken en beveiligen, uitgezonderd de controle van passagiers en bagage op luchthavens[121]

[116] Zie Retsplejeloven voor de typen dwangbevoegdheden: https://www.elov.dk/retsplejeloven/#bog-fjerde-kapitel-71.
[117] Artikelen 780-785 Retsplejeloven.
[118] Databeskyttelsesloven, LOV nr. 502 af 23/05/2018.
[119] De Graaff 2018, p. 98.
[120] Idem.
[121] Bakker & Vos 2023, p 23.

6.2.6 Het nemen en uitvoeren van maatregelen

De PET beslist welke maatregelen worden genomen, op basis van de dreigingsanalyse. De te nemen maatregelen zijn maatwerk. Vervolgens worden deze maatregelen ook door de PET zelf uitgevoerd.

6.2.7 Het evalueren/bijstellen van dreigingsanalyses/maatregelen

Het is niet duidelijk of en hoe de genomen maatregelen (tussentijds) worden geëvalueerd en in welke mate dat kan leiden tot het bijstellen van de dreigingsanalyse en daarmee ook het maatregelenpakket.

6.2.8 Afbouwen van maatregelen

Maatregelen worden door de PET afgebouwd indien uit de evaluatie van de dreigingsanalyse blijkt dat de dreiging niet langer aan de orde is. Op welke wijze maatregelen precies worden afgebouwd is niet bekend.

6.2.9 Toezicht op het stelsel

Uit artikel 13, eerste lid, van de PET-wet volgt dat een natuurlijke persoon of rechtspersoon de Deense Inlichtingencommissie (zoals bedoeld in artikel 16, eerste lid van de PET-wet) kan verzoeken om te onderzoeken of PET zonder rechtvaardiging informatie over de betrokken persoon verwerkt. De Deense Inlichtingencommissie moet nagaan of een grondslag bestaat voor verwerkingen en stelt de betrokken persoon hiervan in kennis. Volgens de toelichting bij de PET-wet wordt in artikel 13 een regeling voor indirecte toegang vastgesteld. De Deense Inlichtingencommissie is de garantie voor de burger dat de PET geen informatie over de burger verwerkt zonder dat daarvoor een rechtvaardiging bestaat. In het kader van deze toegangsregeling kan de Deense Inlichtingencommissie onder meer de PET gelasten informatie te verwijderen die naar het oordeel van de commissie onrechtmatig door de PET wordt verwerkt.[122] De Deense Inlichtingencommissie kan de beoordeling van de PET herzien of de informatie relevant kan worden geacht voor de taken van de dienst.

Uit de wet volgt onder meer dat de bevoegdheid van de Toezichthoudende Raad is uitgebreid tot ook achteraf uitgevoerde wettigheidstoetsingen van de operationele taken van de PET. Volgens de wetsgeschiedenis worden onder “operationele taken” verstaan alle operationele activiteiten die de dienst uitvoert in het kader van de feitelijke uitvoering van zijn taken. Deze worden beschreven in artikel 1 van de PET-wet.

Daarnaast bestaat er een parlementaire commissie, de Commissie voor de Inlichtingendiensten. Uit de wet op de Commissie voor de Inlichtingendiensten[123] volgt dat de commissie aan het begin van elke zittingsperiode wordt benoemd met als doel toezicht te houden op de FE en de PET (artikel 1). De commissie bestaat uit ten minste vijf leden van het parlement, zie artikel 1, lid 2, van de wet op de commissie voor de inlichtingendiensten. Uit artikel 2 van de wet volgt dat de regering de commissie jaarlijks informeert over de activiteiten van de inlichtingendiensten. De commissie kan haar advies over

[122] Pagina 72 van de toelichting bij de PET-wet
[123] Officieel: Lovbekendtgørelse 2014-08-26 nr. 937 om Udvalget vedrørende Efterretningstjenesterne.

de door haar behandelde kwesties mondeling of schriftelijk aan de regering kenbaar maken en kan aan het parlement verslag uitbrengen over haar activiteiten (artikel 3 van de wet).

Met dezelfde Deense wet nr. 160 van 4 juni 2024 werd de rol van de Commissie voor de Inlichtingendiensten verder versterkt.[124] Uit artikel 2a, lid 5, volgt dat de commissie in uitzonderlijke omstandigheden kan besluiten de Deense inlichtingencontrolecommissie te verzoeken specifieke zaken, procedures, kwesties enz. te onderzoeken. Volgens de toelichting bij de wijziging is het doel van de regeling ervoor te zorgen dat de commissie over aanvullende instrumenten beschikt om toezicht te houden op de activiteiten van de inlichtingendiensten.[125]

6.2.10 VIPS

Zoals eerder is besproken behoort tot het takenpakket van de PET ook onder meer het beveiligen en bewaken van het koninklijk huis en van leden van het kabinet. De PET heeft immers als kerntaak het voorkomen en tegengaan van misdrijven tegen de onafhankelijkheid en veiligheid van de staat, alsmede misdrijven tegen de staatsgrondwet en de hoogste staatsautoriteiten. Zo zal de activatie van het stelsel het gevolg zijn van de dreigingsanalyses die de PET maakt, boven op een vorm van basisbescherming die geldt voor VIPS. Omdat het belangrijkste wettelijk kader voor VIPS ook de PET-wet is, verschilt voor zover de deskresearch dat in kaart heeft kunnen brengen het regime niet veel.

Uit artikel 1, lid 1, punt 7, van de PET-wet volgt dat de PET verantwoordelijk is voor de bescherming van personen, organisaties en autoriteiten. Volgens de toelichting bij de PET-wet is PET verantwoordelijk voor de persoonlijke bescherming van de koninklijke familie, met inbegrip van bezoekers van de koninklijke familie, leden van de regering en andere vooraanstaande publieke figuren. De PET moet ook persoonlijke bescherming bieden aan ambassadeurs en bepaalde prominente buitenlandse bezoekers (VIPS) indien nodig.

De nationale politie speelt een ondersteunende rol in het bewaken en beveiligen van personen door samen te werken met de PET. De politie biedt algemene beveiliging en logistieke ondersteuning tijdens openbare evenementen en staatsbezoeken waar hoogwaardigheidsbeklеders aanwezig zijn. Dit omvat verkeersregeling, *crowd management*, en het zorgen voor de algemene openbare orde en veiligheid rond deze evenementen. Voor hoogwaardigheidsbeklеders die onder constante bescherming van de PET vallen, kan de nationale politie extra beveiligingsmiddelen leveren of assisteren bij uitgebreidere beveiligingsmaatregelen. Dit is vooral van belang in situaties waarin de beveiligingseisen de capaciteit of specialisatie van de PET overschrijden.

Uit artikel 4 van de PET-wet volgt dat andere administratieve autoriteiten op verzoek van de PET informatie aan de PET moeten verstrekken als de PET van oordeel is dat de informatie (waarschijnlijk) van belang is voor de uitvoering van de taken van de PET. Volgens de toelichting bij de PET-wet betekent het criterium “waarschijnlijk van belang zijn” dat er een zekere waarschijnlijkheid moet bestaan dat de informatie kan bijdragen tot de uitvoering van de taken van de PET.[126]

---

[124] Officieel: Lov om ændring af lov om Politiets Efterretningstjeneste (PET), lov om etablering af et udvalg om forsvarets og politiets efterre ningstjenester og lov om beskyttelse af whistleblowere.
[125] Bladzijde 31 van de toelichting bij de Wet nr. 160 van 4 juni 2024.
[126] Pagina 60 van de toelichting bij de PET-wet.

Het kader van bevoegdheden van de PET voor informatieverzameling voor het opstellen van de dreigingsanalyse hangt af van het criterium “dat informatie van belang [moet zijn] voor de uitvoering van de taken van PET met betrekking tot de preventie en het onderzoek van strafbare feiten”. We veronderstellen daarom dat die ruimte groter wordt naarmate de staatsveiligheid meer in het gedrang komt. Dat zou dan tot gevolg kunnen hebben dat dreiging tegen bijvoorbeeld de minister(-president) een ruimere bevoegdheid tot informatieverzameling met zich meebrengt. In hoeverre dat daadwerkelijk het geval is, zou onderdeel zijn van de verdiepende studie.

Voor het overige zien we geen aanleiding om aan te nemen dat het bevoegdheidsregime voor VIPS anders is dan zoals hiervoor beschreven voor niet-VIPS.

6.2.11 (Kroon)getuigen

De PET is verantwoordelijk voor de bescherming van (kroon)getuigen in Denemarken. Aangezien de PET het stelsel van bewaken en beveiligen volledig coördineert, is het logisch dat ook de bescherming van (kroon)getuigen onder hun takenpakket valt. Het getuigenbeschermingsprogramma wordt gezien als een laatste redmiddel.[127] Per individuele casus wordt bezien welke maatregelen noodzakelijk zijn de getuigen zo goed mogelijk te kunnen beschermen. Voor getuigen is een aantal verschillende soorten maatregelen mogelijk, zoals het wijzigen van iemands identiteit of verhuizing.[128] Naast getuigen kunnen ook hun families opgenomen worden in het getuigenbeschermingsprogramma en worden maatregelen op hun situatie toegespitst.

6.3 Duitsland

6.3.1 Inleiding

Het stelsel van bewaken en beveiligen is sterk beïnvloed door de Rote Armee Fraktion (RAF). De RAF was een links-extremistische terreurgroep die actief was tussen het eind van de jaren ’60 en de jaren ’90 en die via aanslagen, ontvoeringen en moorden de Duitse staat wilde ondermijnen. Hun geweld, vooral tegen politici en bedrijfsleiders leidde ertoe dat velen in Duitsland bescherming van de staat ontvingen. In de laatste jaren heeft Duitsland te maken gekregen met meerdere incidenten, waarbij verschillende personen het doelwit waren van aanvallen die gelinkt zijn aan rechts-extremisme. Voorbeelden daarvan zijn de moord op de regionale politicus Walter Lübcke in 2019[129], de schietpartijen bij Hanau in 2020 waarbij negen mensen om het leven kwamen[130], en de aanval in Halle in 2019, waarbij een rechts-extremist een synagoge binnen probeerde te dringen en twee mensen doodde toen deze poging niet slaagde.[131] Een recenter incident was de moord op een politieagent in Mannheim, dat in juni 2025 plaatsvond. Dit wakkerde in Duitsland een debat aan over de vraag of er versterking nodig is op het gebied van bewaking en beveiliging van personen, en een verscherping van de wetgeving op dit gebied. Dit incident werd door de Bondskanselier gezien als een terroristische

[127] https://channels.podcastfeed.eu/008dc408-dd22-48f7-976b-c9262ca5396d.
[128] UNODC 2018. Via https://www.unodc.org/documents/treaties/UNCAC/CountryVisitFinalReports/2017_10_21_Denmark_Final_Country_Report.pdf.
[129] https://nos.nl/artikel/2361686-levenslang-geeist-voor-moord-op-cdu-politicus-walter-lubcke.
[130] https://nos.nl/artikel/2323881-aanslag-hanau-gevolg-van-groei-rechts-extremisme-in-duitsland.
[131] https://nos.nl/artikel/2305381-zeker-twee-doden-bij-aanslag-in-duitse-stad-halle-verdachte-opgepakt.

aanval.[132] In Duitsland is extra aandacht voor het bewaken en beveiligen van Joodse instellingen, risico's rondom kerstmarkten en dreigingen ten aanzien van bepaalde bevolkingsgroepen en geloofsgemeenschappen. Daarnaast wordt Duitsland geconfronteerd met anti-overheidssentiment onder een deel van de bevolking en dat consequenties kan hebben voor het bewaken en beveiligen van personen. In Duitsland is in mindere mate sprake van dreigingen vanuit de georganiseerde misdaad, zeker in vergelijking met Nederland. Dit geldt ook voor de deelstaat Nedersaksen. Dit hoofdstuk beschrijft het algemene stelsel op bondsniveau en de situatie in Nedersaksen in het bijzonder.

6.3.2 Rolverdeling en verhouding tussen betrokken organisaties

Duitsland bestaat uit een federale overheid en zestien deelstaten. Het stelsel van bewaken en beveiligen is een samenspel van federale en lokale autoriteiten die met elkaar samenwerken, maar specifieke eigen taken hebben. Het centraal domein is de verantwoordelijkheid van de Bundeskriminalamt (hierna: BKA), het decentraal domein wordt in de deelstaten zelfstandig uitgevoerd door de politie van de deelstaat. Hoewel de decentrale autoriteiten zelfstandige bevoegdheden hebben wordt er vanuit het Bundesniveau sterk gestuurd op een uniforme werkwijze tussen de deelstaten.[133] Deze centrale aansturing is verankerd in het (niet-openbare) voor alle deelstaten geldende Polizeidienstvorschrift 129. De betrokken organisaties zijn de federale politie (in het bijzonder de BKA, de politie van de verschillende deelstaten en de Duitse binnenlandse en buitenlandse inlichtingendiensten (Bundesamt für Verfassungsschutz (BfV) en Bundesnachrichtendienst (BND)). Daarnaast is er nog een specifieke eenheid die zowel onderdeel is van de federale als de deelstaatpolitie, de 'Personenschutzkommandos'. Binnen het stelsel van bewaken en beveiligen wordt een onderscheid gemaakt tussen taken die onder verantwoordelijkheid van de federale overheid vallen en taken die tot de verantwoordelijkheid van de deelstaten behoren.

Taken op federaal niveau

De federale taken op het gebied van bewaken en beveiligen zijn een verantwoordelijkheid van het BKA en daarmee van de Bondsminister van Justitie en Veiligheid. De federale overheid heeft alleen een speciale bevoegdheid voor een strikt gedefinieerde groep personen in de wet. Zo is de bescherming van de leden van de constitutionele organen van de Federatie een taak van het BKA.[134] Het gaat hierbij om het bewaken en beveiligen van federale gezagsdragers en objecten, zoals federale ministeries en bijvoorbeeld de Deutsche Bank. De afdeling Sicherungsgruppe (SG) van het BKA waarborgt de persoonsbeveiliging van de Bondspresident, leden van de Bondsdag en de Bondsraad, het Federaal Constitutioneel Hof en de federale regering, evenals hun buitenlandse gasten.

Een belangrijke functie van het BKA is het beoordelen van de dreigingsniveaus tegen personen die zij beschermen. Deze analyses zijn gebaseerd op inlichtingen verzameld door het BKA en andere inlichtingendiensten, al wordt in ander onderzoek geconcludeerd dat deze samenwerking minder sterk is georganiseerd.[135] De uitkomsten van deze analyses bepalen de intensiteit en aard van de

[132] https://www.bundesregierung.de/breg-en/federal-government/federal-chancellor-government-statement-security-situation-2290986.
[133] Dit wordt onder meer geregeld in de Zeugenschutzharmonisierungsgesetz (ZSHG).
[134] https://www.polizei-dein-partner.de/service/praevention-kompakt.html/.
[135] Bakker & Vos 2023, p. 13.

beveiligingsmaatregelen die worden ingezet. De BKA neemt deze maatregelen zelf. Het BKA heeft ten slotte een coördinerende rol in het verschaffen van deze informatie aan relevante betrokken partijen om op die manier de integrale aanpak te kunnen waarborgen.

Personenschutzkommandos bieden directe fysieke beveiliging aan personen die onder hun bescherming staan. Hun primaire taak is het beschermen van hooggeplaatste ambtenaren, politieke leiders, buitenlandse dignitarissen en andere individuen die vanwege hun positie of specifieke dreigingen een verhoogd risico lopen. Dit omvat het begeleiden van de beschermde personen naar verschillende locaties, het zorgen voor hun veiligheid tijdens evenementen, en het implementeren van beveiligingsprotocollen om hun veiligheid te allen tijde te garanderen. Deze eenheden voeren ook risicoanalyses uit om de dreigingsniveaus voor de personen die zij beschermen te bepalen. Het belangrijkste verschil tussen het BKA en de Personenschutzkommandos ligt in hun scope en focus. Het BKA heeft een bredere, meer strategische rol die nationale en internationale veiligheidskwesties omvat, terwijl de Personenschutzkommandos zich specifiek richten op de directe, operationele aspecten van het bewaken en beveiligen op federaal niveau.

Opvallend is overigens dat het BKA heeft aangekondigd dat het aantal persoonlijke beveiligingsfunctionarissen voor toppolitici in 2025 en 2026 zal worden verhoogd van 500 naar 700. De reden hiervoor is de toegenomen dreigingssituatie. De toegenomen gevaarsituatie komt mede voort vanwege ontwikkelingen in Oekraïne en de oorlog in Gaza.

Taken op deelstaatniveau

Elke Duitse deelstaat heeft eigen politiewetten die de taken en bevoegdheden van hun politiediensten specificeren. Alle beveiligingstaken die niet behoren tot de beveiligingstaak op federaal niveau zijn toebedeeld aan de deelstaten onder verantwoordelijkheid van de minister van Binnenlandse Zaken van de deelstaat. Dit betreffen de gevallen waarbij lokale politici en ambtenaren van de deelstaat, journalisten of anderen die risico lopen op basis van hun functie, activiteiten of werkzaamheden betrokken zijn. De beveiligingstaken worden uitgevoerd door de lokale politie. In Duitsland wordt het onderscheid tussen gezag en uitvoering niet gemaakt. De politie vormt zowel het gezag als de uitvoering en staat onder directe aansturing van de minister van Binnenlandse Zaken van de deelstaat. Op deelstaatniveau bepaalt de politie de aard en ernst van de dreiging en of persoons- of objectbeveiliging nodig is en welke maatregelen getroffen moeten worden. Dit kan bijvoorbeeld bestaan uit persoonsbeveiliging, bewaking van woningen of werkplekken, en escortes voor veilige verplaatsingen. Ook voert de deelstaatpolitie haar eigen dreigingsanalyses uit met betrekking tot de lokale omstandigheden.

Bewaken en beveiligen in Nedersaksen

Het Landeskriminalamt (LKA) Niedersachsen is verantwoordelijk voor het bewaken en beveiligen van personen op deelstaatsniveau. Het LKA is onderverdeeld in zes Abteilungen (afdelingen) en elke Abteiling is onderverdeeld in Dezernaten (diensten), elk met een specifieke taak. Dienst 25 van afdeling 2 van het LKA is specifiek belast met Zeugenschütz en Operativer Opferschütz: getuigenbescherming (in strafzaken) en Opferschütz (zgn. slachtofferbescherming en vormt daarmee een restcategorie van te beschermen personen). Het bewaken en beveiligen van personen in Nedersaksen is aldus geregeld binnen één gespecialiseerde organisatie-eenheid van het LKA en is daarbij verantwoordelijk voor zowel uitvoering als coördinatie.

De bescherming van andere doelgroepen, zoals bijvoorbeeld bedreigde journalisten, is eveneens de taak van dienst 25 van de LKA en is geregeld in de (niet-openbare) Richtlijn voor operationele slachtofferbescherming. De beschermingsmaatregelen die getroffen kunnen worden zijn vrijwel identiek aan maatregelen voor getuigenbescherming. De vraag of iemand al dan niet gevaar loopt, wordt beantwoord aan de hand van criteria die zijn vastgelegd in de (niet-openbare) Regeling Politiediensten (PDV) 129. De beschermingsmaatregelen worden uitgevoerd door medewerkers van dienst 25.[136] De verantwoordelijkheid voor het beschermen van personen is een '*Kooperationskonzept zwischen Fachberatungsstellen* (dienst 25) *und Polizei*'.[137]

6.3.3 Aanleiding inzet van het stelsel

Het stelsel kan inwerkingtreden door middel van aangifte. De eerste risicobeoordeling wordt gemaakt door de politiemedewerker die de aangifte opneemt. Politiemedewerkers zijn opgeleid om een eerste risicobeoordeling te kunnen maken. Ook kan ambtshalve het proces in werking worden gesteld. Als er een mogelijk risico wordt vastgesteld, wordt de aangifte voorgelegd aan de opsporing alwaar een tweede beoordeling plaatsvindt. De casus wordt vervolgens ingeschaald in één van de vier mogelijke categorieën: 1) erg groot risico, 2) groot risico en 3) weinig risico of 0) geen risico. Als de casus in categorie 1 of 2 wordt ingeschaald, dan wordt de casus overgedragen aan de Personenschutz van dienst 25. Daar wordt de casus opnieuw beoordeeld, wordt een dreigingsinschatting gemaakt en worden maatregelen geadviseerd. De politie-informatie is hierbij leidend. Iedere zes maanden wordt standaard een nieuwe risico-inschatting gemaakt. De maatschappelijke status of het beroep van de bedreigde persoon heeft daarentegen in principe geen invloed op de politiewerkwijze en standaardmaatregelen. Deze kunnen variëren van een gerichte bewustmaking, gesprekken met de bedreiger of de bedreigde persoon, een tijdelijke inbewaringneming tot opname in het getuigenbeschermingsprogramma.[138]

6.3.4 Dwangbevoegdheden voor informatieverzameling en dreigingsanalyses

In Duitsland is er een nauwe samenwerking tussen de domeinen van bewaken en beveiligen en opsporing, zowel op federaal als op deelstaatniveau. Met name waarbij het gaat om de inschatting van dreigingen. Het Duitse openbaar ministerie heeft geen taak in bewaken en beveiligen, alleen bij het verlenen van toestemming om politie-informatie te gebruiken die is verkregen tijdens strafrechtelijke onderzoeken.

De Duitse binnenlandse veiligheidsdienst (BfV) speelt in het kader van het leveren van inlichtingen voor het bewaken en beveiligen van personen eveneens een voorname rol. De BfV voert (preventieve) gedetailleerde dreigingsanalyses uit om te bepalen welke personen of groepen mogelijk risico lopen op basis van informatie over geplande of potentiële aanvallen. Het biedt adviezen en waarschuwingen aan andere veiligheidsdiensten, zoals het BKA en de deelstaatpolitie, over specifieke dreigingen die kunnen vereisen dat bepaalde personen extra bescherming nodig hebben.

[136] Informatie aangereikt door LKA Niedersachsen.
[137] LKA 2025.
[138] Informatie aangeleverd door LKA Niedersachsen.

De bevoegdheden om informatie te verzamelen zijn neergelegd in wetgeving op federaal en deelstaatniveau. Qua federale wetgeving is het Strafprozeßordnung (wetboek van Strafvordering) van toepassing. Op deelstaatniveau zijn bevoegdheden geregeld in het Gefahrenabwehrrecht (NPOG).

De Duitse buitenlandse inlichtingendienst (BND) verzamelt inlichtingen uit verschillende landen en analyseert deze om Duitsland te waarschuwen voor mogelijke internationale bedreigingen die invloed kunnen hebben op Duitse burgers en belangen in het buitenland.

In Nedersaksen hebben degenen binnen dienst 25 van het LKA die verantwoordelijk zijn voor het opstellen van dreigingsanalyses zelfstandig wettelijke bevoegdheden om informatie te vergaren om tot bruikbare dreigingsanalyses te komen. Dit is geregeld in het Gefahrenabwehrrecht (NPOG).

6.3.5 Het delen van informatie tussen betrokken organisaties

In de Wet op de Federale Politie (Bundespolizeigesetz, BPolG) zijn de taken en bevoegdheden van de Bundespolizei vastgelegd. De wet bevat bepalingen over samenwerking en informatie-uitwisseling met andere politiediensten. Verder kent elke deelstaat zijn eigen politiewetten waarin zowel de bevoegdheden als de structuur van de politieorganisatie is geregeld en waarvoor en onder welke omstandigheden informatie kan worden uitgewisseld. Binnen de politie kan de informatie-uitwisseling onbeperkt plaatsvinden.[139]

6.3.6 Het nemen en uitvoeren van de maatregelen

De juridische basis voor persoonsbescherming is landelijk vastgelegd in *Polizeidienstvorschrift 129. (PDV 219).* In dit niet-openbare document worden zowel risicobeoordeling als de mogelijke maatregelen die daarop getroffen kunnen worden in detail beschreven.

De Wet op de Federale Politie regelt de taken en bevoegdheden van de federale politie in Duitsland. Daarnaast is er voor BKA een specifieke BKA-wet, waarin de taak om de eerdergenoemde personen te beschermen is vastgelegd. Wat betreft de deelstaatpolitie, heeft elk van de 16 deelstaten in Duitsland zijn eigen politiewet die de bevoegdheden en verantwoordelijkheden van de politie op deelstaatniveau regelt, inclusief de beveiliging van personen. Deze wetten specificeren wanneer en hoe de politie mag optreden om personen te beschermen tegen bedreigingen. Er zijn verschillende gradaties van maatregelen die getroffen kunnen worden om bescherming te verlenen aan de bedreigde persoon.[140] De uitvoering van de maatregelen berust bij medewerkers van Dienst 25. Zij kunnen worden ondersteund door eenheden van de politie.

6.3.7 Het evalueren/bijstellen van dreigingsanalyes/maatregelen

Iedere zes maanden wordt standaard een nieuwe risico-inschatting gemaakt. In gevallen zoals eerwraak worden specialisten/wetenschappers ingeschakeld ter advisering. Het gehele proces is gedetailleerd beschreven in het niet-openbare (nur für Dienstgebrauch) *Polizeidienstvorschrift 129.*

[139] Informatie aangereikt door LKA Niedersachsen.
[140] Idem.

6.3.8 Afbouwen van maatregelen

Als uit de halfjaarlijkse periodieke risico-inschatting blijkt dat er geen gevaren meer zijn die bescherming noodzakelijk maken wordt besloten tot het afbouwen of opheffen van de maatregelen.

6.3.9 Toezicht

Intern toezicht vindt plaats door de directie van het LKA. Externe controle wordt op permanente basis uitgevoerd via de parlementaire evaluatie van de relevante wetten en op het gebied van de gegevensoverdracht. Toezicht op individuele gevallen gebeurt op basis van onderzoek door een parlementaire controlecommissie.[141]

6.3.10 VIPS

Het beschermen van VIPS valt onder verantwoordelijkheid van het BKA. Een gelimiteerd aantal personen ontvangt ambtshalve bescherming (zie paragraaf 7.3.2.).

6.3.11 (Kroon)getuigen

De voorwaarden om toegelaten te worden tot het getuigenbeschermingsprogramma zijn vastgelegd in paragraaf 1 van de Zeugenschutzharmonisierungsgesetz.[142] Dit is een federale wet die de regels en procedures voor de bescherming van getuigen in strafrechtelijke procedures binnen Duitsland uniformeert. De toelatingseisen voor getuigenbescherming zijn daardoor in alle deelstaten hetzelfde.

Iemand wordt toegelaten tot het getuigenbeschermingsprogramma in geval:

- Er sprake is van een ernstig misdrijf, in het bijzonder een terroristisch misdrijf
- Van een aanzienlijk belang voor de verklaring van de getuige voor de strafprocedure
- Bescherming noodzakelijk is voor de volledige bereidheid van de getuige om te getuigen
- Het bestaan van directe aanwijzingen voor gevaar van leven, ledematen, gezondheid, vrijheid of belangrijke bezittingen als gevolg van het besluit om te getuigen
- Er sprake is van vrijwillige deelname aan het getuigenbeschermingsprogramma
- De getuige geschikt is voor treffen van beveiligingsmaatregelen

Wanneer een dreigingssituatie wordt vastgesteld wordt er een verzoek tot opname gedaan voor de te beschermen persoon in het getuigenbeschermingsprogramma. De daaropvolgende beschermingsmaatregelen voor deze persoon worden primair uitgevoerd door de medewerkers van de getuigenbeschermingsdienst (dienst 25). Personen die gevaar lopen, worden daar in de eerste plaats begeleid door getuigenbeschermers van deze dienst, waarbij ook andere eenheden van de politie van Nedersaksen ondersteunend kunnen optreden. Hierbij kan gedacht worden aan ondersteuning van de politie tijdens rechtszittingen met een hoog risico.

[141] Informatie aangereikt door de LKA Niedersachsen.
[142] https://www.gesetze-im-internet.de/zshg/.

6.4 Frankrijk

6.4.1 Inleiding

De afgelopen jaren heeft Frankrijk te maken gehad met een aantal grote terroristische aanslagen en dreigingen zoals de aanslag op Charlie Hebdo in 2015 en zes andere aanslagen die in november van dat jaar gepleegd werden.[143] Als reactie hierop werd de noodtoestand uitgeroepen en de beveiliging in het land sterk aangescherpt. Door de noodtoestand kreeg de politie vergaande bevoegdheden, bijvoorbeeld om zonder machtiging huiszoekingen te doen. De maatregelen stuitten op veel kritiek; critici benoemden dat Frankrijk verder ging dan noodzakelijk en in een politiestaat veranderde.[144] Ook in de periode rondom de Olympische Spelen zijn zware beveiligingsmaatregelen genomen waarbij vergaande inzet van vergaande bevoegdheden plaatvond en waarbij volop werd ingezet op surveillance en monitoring, zoals gezichtsherkenningstechnologie en het observeren van gedrag met behulp van kunstmatige intelligentie. Experts waarschuwden destijds al voor het risico dat deze techniek ook na de Spelen zou worden ingezet.[145] De wetswijziging die het gebruik van veiligheidscamera´s toeliet bleef inderdaad nog van kracht tot maart 2025.

6.4.2 Rolverdeling en verhouding tussen betrokken organisaties

Bij de bewaking van bedreigde personen zijn de volgende organisaties betrokken: de Unité de Coordination de la Lutte Antiterroriste, het ministerie van Binnenlandse zaken, de prefect, de Nationale Politie, specifiek de *Service de La Protection*, de Franse veiligheidsdiensten, de *Gendamerie en* de *Police Municipale*.

Voor het inschatten van dreigingen zijn de veiligheidsdiensten en andere onderdelen van de nationale politie betrokken. Als er sprake is van terrorismedreiging, dan is het coördinerende orgaan Unité de Coordination de la Lutte Antiterroriste (hierna: UCLAT) betrokken bij de dreigingsanalyse.

De minister van Binnenlandse Zaken is verantwoordelijk voor de beveiliging van personen en gaat over het beoordelen en toekennen van de beveiligingsmaatregelen. Op lokaal terrein is de prefect, een hoge ambtenaar die de staat vertegenwoordigt (zie artikel 72, lid 6 Franse Grondwet), betrokken bij de besluitvorming en de coördinatie van de politiediensten. Binnen zijn departement heeft de prefect namelijk gezag over de politie en de Gendamerie. De Gendarmerie is een militaire politiemacht en valt onder de verantwoordelijkheid van het ministerie van Defensie. De precieze rolverdeling tussen de minister en de verschillende prefecten is niet duidelijk.[146]

De Service de la Protection (hierna: SDLP) biedt voornamelijk beveiliging aan mensen met een hoog dreigingsrisico.[147]

---

[143] In 2024 daalde het aantal terreurdreigingen, maar vernieuwde dreigingen zorgen ervoor dat het land op haar hoede moet blijven, zie ook Rodde 2025. Via https://hal.science/hal-04946412v1/file/Research_Note_CREOGN_110_Terrorism_French_Extremism_Movements_2024_2-1.pdf.

[144] https://decorrespondent.nl/4207/waarom-de-fransen-liever-in-een-veiligheidsstaat-dan-in-een-democratie-lijken-te-willen-leven/97bbcd84-1ed9-0e98-3e12-0e85f3ce40af.

[145] https://www.volkskrant.nl/buitenland/als-het-olympische-circus-uit-parijs-is-vertrokken-blijven-de-surveillance-camera-s-gewoon-hangen~b47e31e0/?.

[146] https://www.eurometropolis.eu/nl/frans-belgische-gids-over-de-instellingen-en-bevoegdheden/frankrijk/de-franse-staat.

[147] Arrêté du 12 août 2013 relatif aux missions et à l'organisation du service de la protection.

Voor de overige gevallen wordt de beveiliging uitgevoerd door de Nationale Politie in de stedelijke gebieden) en de *Gendarmerie*, voornamelijk in de niet-stedelijke gebieden.

De *Police Municipale* (de gemeentepolitie) heeft geen voorname eigenstandige rol in het beschermen en bewaken van personen in Frankrijk, maar kan wel ondersteuning bieden aan gespecialiseerde diensten op operationeel niveau. Als er sprake is van minder ernstige dreigingen, of situaties waarin geen onmiddellijk nationale veiligheidsdreiging bestaat, kunnen lokale politieautoriteiten betrokken zijn bij het uitvoeren en nemen van beslissingen over persoonsbeveiliging, met name als het gaat om lokale ambtenaren, evenementen of getuigen in hun gebied. Gemeentelijke politieambtenaren vallen onder het gezag van de burgemeester.[148]

6.4.3 Aanleiding inzet van het stelsel

Een aangifte van de bedreigde persoon kan aanleiding zijn om het stelsel in te zetten. Of er verder andere aanleidingen mogelijk zijn is niet bekend.

6.4.4 (Dwang)bevoegdheden voor informatieverzameling en dreigingsanalyses

Dreigingen vanuit georganiseerde misdaad

Analyses van dreigingen vanuit de georganiseerde criminaliteit worden opgesteld door afdelingen van de nationale politie en de *Gendamerie* die zich bezighouden met de bestrijding van verschillende vormen van georganiseerde criminaliteit. Zo voert de *Sous-direction de la Lutte contre la Criminalité organisée* (SDLC) de analyse uit bij bedreiging door maffianetwerken, drugskartels en wapensmokkel en de *Office Central pour la Répression du Banditisme* (ORCB) bij gewelddadige criminelen. Hoe deze analyses er precies uitzien is niet bekend. De inzet van bevoegdheden voor informatievergaring volgen uit de bevoegdheden die de politie heeft in geval van de opsporing van strafbare feiten.[149]

Dreigingen vanuit terrorisme

Als er sprake is van een dreiging vanuit terrorisme is de werkwijze als volgt. Frankrijk kent een inlichtingen- anti-terrorismeverband*, La coordination nationale du renseignement et de la lutte contre le terrorisme,* waarbij het mogelijk is gemaakt voor de inlichtingendiensten om beleid tegen dreigingen gezamenlijk en efficiënter uit te voeren.[150] Het regelt de coördinatie van de verschillende inlichtingendiensten en tevens het beheer van alle diensten die zich inzetten tegen terrorisme (inlichtingendiensten, gerechtelijke politiediensten en diensten van het ministerie van Justitie).

Een van de belangrijkste organisaties die informatie vergaart en dreigingsanalyses opstelt in geval van terroristische dreigingen is de *Direction générale de la sécurité intérieure* (hierna: DGSI). Op basis hiervan kan de DGSI adviezen uitbrengen over specifieke beveiligingsmaatregelen. De DGSI werkt binnen een juridisch kader voor specifieke doeleinden waarop controle wordt uitgevoerd: de Code de la sécurité intérieure (hierna: Code de la sécurité).[151]

---

[148] https://www.policemunicipale.fr/connaitre/competence/.
[149] Code de la sécurité intérieure.
[150] https://www.elysee.fr/cnrlt.
[151] https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/notre-cadre-legal/fondements.

De DGSI kan ook betrokken zijn bij preventieve acties, om dreigingen te neutraliseren, door het volgen van personen, het onderscheppen van communicatie en andere surveillance-activiteiten. In geval van een acute dreiging of een beveiligingsincident, speelt de DGSI een rol in het crisismanagement, door te helpen bij het coördineren van de reactie op incidenten die de veiligheid van beschermde personen beïnvloeden. Het DGSI valt onder het ministerie van Binnenlandse Zaken.

De *Unité de coordination de la lutte antiterroriste* (hierna: UCLAT) speelt een centrale rol in de terrorismebestrijding in Frankrijk, en is vooral belangrijk bij het coördineren van informatie-uitwisseling en dreigingsanalyses — ook in relatie tot persoonsbeveiliging. De UCLAT, die in 2020 als eenheid is ondergebracht bij DGSI, is een centrale coördinatie-eenheid die informatie verzamelt en analyseert uit álle betrokken diensten en werkt ten behoeve van álle uitvoerende instanties.[152]

De UCLAT concludeert hoe groot een dreiging is en of deze acuut is of niet. De UCLAT adviseert andere organisaties, bijvoorbeeld de politiedienst die persoonsbeveiliging uitvoert, over welke maatregelen genomen moeten worden en coördineert de acties van verschillende diensten.[153] Naast deze tactische producten, maakt de UCLAT ook strategische beelden; bijvoorbeeld hoe dreigingsfenomenen zich ontwikkelen. De analyses helpen bij het vormen van beleid en operationele beslissingen over hoe en waar beveiligingsmiddelen het best kunnen worden ingezet. De UCLAT helpt bij het ontwikkelen van strategieën en tactieken om terrorisme effectief te bestrijden, inclusief preventieve maatregelen om individuen en groepen te beschermen tegen terroristische aanslagen.

De procedure die de UCLAT volgt om tot een product te komen ziet er als volgt uit:

1. Start op eigen initiatief of door verwijzing door minister naar de UCLAT van een bepaald evenement of persoon de opdracht voor een risico- en dreigingsanalyse;

2. Franse partnerdiensten worden bevraagd naar wat zij hebben liggen op deze persoon, of dit evenement;

3. Informatie uit de eigen database en van bijvoorbeeld sociale media wordt toegevoegd;

4. Beeld wordt gevormd, product wordt gemaakt en gedeeld met de bevoegde dienst voor persoonsbeveiliging. In theorie is het mogelijk om een (andere) dienst tot vergaring van nieuwe informatie over te gaan, en daarvoor een menselijke bron te gebruiken. Het kabinet van de minister van Binnenlandse zaken besluit over met wie het product gedeeld wordt.

De UCLAT maakt twee verschillende producten: risico- en dreigingsanalyses, welke zien op de karakteristieken en het gedrag van respectievelijk de te beveiligen persoon en het bedreigende fenomeen. De schattingen lopen op een schaal van 4 (geen dreiging), 3 (latente dreiging), 2 (imminente dreiging) tot 1 (dreiging in uitvoering).

In het kader van bewaken en beveiligen worden in geval van dreiging, door de UCLAT de bestuurlijke autoriteiten gewaarschuwd. Deze kunnen vervolgens concrete maatregelen nemen. Op de UCLAT rust geen plicht om de bestuurlijke autoriteiten te waarschuwen.

---

[152] https://www.dgsi.interieur.gouv.fr/decouvrir-dgsi/nos-missions/lutte-contre-terrorisme-et-extremismes-violents/dgsi-chef-de-file-en.
[153] https://www.cf2r.org/wp-content/uploads/2017/05/UCLAT.pdf.

De producten voor afnemers worden *note blanche* genoemd. Op basis hiervan kunnen maatregelen worden genomen. In geval van een dreiging waarschuwt de UCLAT de bestuurlijke autoriteiten.

Informatieverzameling op basis van openbare bronnen, andere organisaties en dwangbevoegdheden

De Franse veiligheidsdiensten hebben specifieke, in de wet vastgelegde dwangbevoegdheden voor het verzamelen van informatie in het kader van de bewaking en beveiliging van personen als er sprake is van een terroristische dreiging.

De Code de la sécurité Intérieure schept bevoegdheden zoals het nemen van preventieve maatregelen en beveiligingszones, voor surveillance en monitoring, het onderscheppen van communicatie en het inzetten van noodbevoegdheden. Ook is een hoofdstuk gewijd aan de inlichtingendiensten.

Ook het verzamelen van informatie via andere organisaties is vastgelegd. Een specifiek artikel dat betrekking heeft op het delen van informatie, is artikel R232-15. Dit artikel bepaalt welke functionarissen gemachtigd zijn om binnen de grenzen van hun bevoegdheden en taakstelling informatie te ontvangen van andere diensten. In de annex van de Code de la Sécurité zijn daarnaast regels opgenomen over het delen van gegevens tussen het hoofd van de Staatsveiligheidsdiensten en de gemeentelijke politie.[154]

De geautomatiseerde verwerking van gegevens is geregeld in de artikelen L232-1 tot en met L235-1. Deze artikelen hebben als doel het voorkomen de van bepaalde terroristische misdrijven, aanslagen en specifiek benoemde feiten neergelegd in bijlage II van de Richtlijn (EU) 2016/681 en het Franse Wetboek van Strafvordering. De artikelen creëren een wettelijke basis voor het verwerken van gegevens door de Minister van Binnenlandse Zaken, de Minister van Defensie, de Minister van Transport en de Minister van Douane. De geautomatiseerde verwerking van voertuiggegevens kan ook uitgevoerd worden door de nationale politie-, douane- en gendarmeriediensten. In hoofdstuk 8 is meer informatie vastgelegd over het verzamelen van informatie door inlichtingendiensten. Zo bepaalt artikel L863-2 dat overheidsdiensten anders dan inlichtingendiensten op verzoek van aangewezen diensten alle informatie delen als dat noodzakelijk is voor de nationale veiligheid.[155]

De loi relative à la sécurité intérieure et à la lutte contre le terrorisme (Wet op de binnenlandse veiligheid en terrorismebestrijding) is ontworpen om het wettelijk kader voor terrorismebestrijding te versterken en te formaliseren. Deze wet, die in 2017 werd aangenomen, heeft als doel de autoriteiten effectieve middelen te bieden om de openbare veiligheid te handhaven en tegelijkertijd de grondwettelijke vrijheden te respecteren. Belangrijk is dat de wet de politie uitgebreidere bevoegdheden geeft om informatie te verzamelen, met name via elektronisch toezicht en andere surveillance-technieken, om potentiële terroristische bedreigingen proactief te identificeren en te monitoren.

De loi relative au renseignement, die onderdeel uitmaakt van de Code de la Securité, regelt de verantwoordelijkheden van Franse inlichtingendiensten. De wet uit 2015 heeft – ook in het licht van

---

154 https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000028286312/#LEGISCTA000028286537.

155 Artikel L811-2 van de Code de la sécurité wijst die diensten aan.

de verschillende terroristische dreigingen die Frankrijk in de afgelopen jaren heeft meegemaakt[156] – de dwangbevoegdheden van inlichtingendiensten uitgebreid, vooral vergeleken met het Franse equivalent van de Telecommunicatiewet uit 1991 die als wettelijk kader diende.[157] Die wet bepaalde dat inlichtingendiensten communicatie mochten aftappen op bevel van de minister (artikelen 3 en 4). Voor draadloze communicatie mocht dit zelfs zonder enige beperking (artikel 20).[158]

Voor wat betreft data gelden specifieke bewaringstermijnen voor inlichtingendiensten.[159] De inhoud (*correspondances)* mag 1 maand na het verzamelen van de data bewaard worden, de metadata 4 jaar. De periode begint bij versleutelde content na decodering. Dit moet binnen 6 jaar na verzameling gebeuren. Voor internationale inlichtingen zijn deze periodes langer: 1 jaar en 6 jaar respectievelijk.

6.4.5 Het delen van informatie tussen betrokken partijen

Het delen van informatie tussen betrokken is alleen bekend wat betreft het geval er sprake is van een terroristische dreiging.

De Code de la sécurité bevat bepalingen die een basis bieden voor online informatievergaring in het kader van terrorismebestrijding in relatie tot het waken over de veiligheid van personen. Hierin zijn bepalingen opgenomen die de samenwerking en informatie-uitwisseling tussen verschillende veiligheidsdiensten reguleren.

In 2018 is de wet herzien om de data-uitwisseling tussen de Franse inlichtingendiensten te vereenvoudigen. Analisten kunnen met behulp van 'selectoren' of 'indicatoren' die overeenkomen met personen die zich in het buitenland bevinden, de databases van Frankrijk doorzoeken op metadata.[160] Hiermee kan een 'sociale grafiek' worden vastgesteld en potentiële verdachten in Frankrijk identificeren, met maatregelen als monitoring ter gevolg.

6.4.6 Het nemen en uitvoeren van maatregelen

De Minister van Binnenlandse zaken beslist op basis van de dreigingsanalyse(s) of iemand in aanmerking komt voor bewaking en welke maatregelen daarbij moeten worden genomen.[161] Hiervoor krijgt hij advies van een commissie waarin de directeur-generaal van de nationale politie, de directeur-generaal van de nationale gendarmerie, de prefect van de Parijse politie, het hoofd van de beschermingsdienst en de directeur-generaal van de interne veiligheid deelnemen. Indien noodzakelijk kan de Minister ook beveiligingsmaatregelen nemen zonder de commissie te consulteren. Vervolgens worden de maatregelen uitgevoerd door de betreffende politiedienst die is belast met de bewaking van de betreffende persoon.

6.4.7 Het evalueren/bijstellen van dreigingsanalyses/maatregelen

Bij wijzigingen in de situatie worden dreigingsanalyses bijgesteld door de betrokken dienst die de analyse heeft uitgevoerd. Wat betreft terrorisme dreigingen staat UCLAT in dagelijks contact met de

[156] Deze regelgeving is een reactie op de Charlie Hebdo aanval.
[157] Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.
[158] https://www.europarl.europa.eu/doceo/document/A-5-2001-0264-PAR01_NL.pdf, p.92
[159] Loi n°2018-607 du 13 juillet 2018, article 37.
[160] Tréguer 2021. Via https://shs.hal.science/halshs-01399548/document.
[161] Art. 5 Arrêté du 12 août 2013 relatif aux missions et à l'organisation du service de la protection.

afnemers van haar producten om te zien hoe de implementatie van het product verloopt en om te bezien of dreigingsinschattingen aangepast dienen te worden. Op basis hiervan wordt bezien of maatregelen bijgesteld moeten worden.

6.4.8 Het afbouwen van maatregelen

Maatregelen worden afgebouwd op basis van nieuwe inzichten uit de dreigingsanalyse. Het is niet bekend op welke wijze maatregelen precies worden afgebouwd. Aannemelijk is dat dit proces vergelijkbaar is met het proces waarmee de minister van Binnenlandse Zaken beslist welke maatregelen worden genomen.

6.4.9 Toezicht op het stelsel

Met de inwerkingtreding van de Code de la Securité als overkoepelend wettelijk kader voor alle bevoegdheden op het terrein van de binnenlandse veiligheid is de onafhankelijke *Commission nationale de contrôle des techniques de renseignement* (hierna: CNCTR) ingesteld. Aangezien inlichtingendiensten bevoegdheden kunnen inzetten om informatie te vergaren, kan dit op gespannen voet staan met privacyvraagstukken. De CNCTR adviseert hierin.[162] Jaarlijks brengt de CNCTR ook een rapport uit waarin wordt ingegaan op de inzet van inlichtingentechnieken en formuleert zij aanbevelingen om het overzicht en de monitoring hierop te verbeteren.[163]

Dit adviesorgaan bestaat uit:

- vier parlementsleden, aangewezen door de voorzitters van beide kamers van het parlement;
- twee administratieve rechters en twee rechterlijke rechters, respectievelijk aangewezen door de Raad van State en de Cour de Cassation;
- een technisch expert, aangewezen door de nationale telecomtoezichthouder (de toevoeging van een commissaris met technische expertise was de belangrijkste vernieuwing).

De CNCTR heeft 24 uur de tijd om een voorafgaand, niet-bindend advies uit te brengen over de surveillancevergunningen die door de premier worden verleend voordat de surveillance begint. In gevallen van "absolute noodzaak" wordt de commissie echter enkel op de hoogte gesteld van de maatregel binnen 24 uur na afgifte (artikel L. 821-3). Ook ex-ante kan advies worden uitgebracht.[164]

Voor toezicht achteraf heeft de CNCTR "permanente, volledige en directe toegang tot dossiers, logs, verzamelde inlichtingen, transcripties en extracties" van de verzamelde gegevens. Het kan zowel geplande controles uitvoeren als controles op locatie, waar deze documenten gecentraliseerd worden bewaard (artikel L. 833-2-2). Als er een onregelmatigheid wordt vastgesteld, kan de CNCTR een "aanbeveling" sturen naar de premier met het verzoek om deze te beëindigen.

---

[162] https://www.cnctr.fr/en/mission.
[163] Présidence de la République 2025. Via https://www.elysee.fr/admin/upload/default/0001/17/5c505c864b51263567a46ec7647e7199fad868d6.pdf.
[164] https://www.cnctr.fr/

6.4.10 VIPS

Een VIP in Frankrijk heeft recht op beveiliging zodra deze persoon een van de beschermde functies bekleedt. Het stelsel wordt dus op basis van functies geactiveerd.

In Frankrijk is een aantal functies aangewezen die standaard beveiliging krijgen. Het gaat om de minister-president, de premier en de minister van Binnenlandse Zaken, de minister van Defensie en de minister van Buitenlandse Zaken.[165] Buitenlandse regeringsleiders en staatshoofden die een bezoek aan Frankrijk brengen vallen hier ook onder. Voor overige buitenlandse functionarissen geldt dat beveiliging wordt ingezet als een vooraf gemaakte dreigingsanalyse daartoe aanleiding geeft.[166]

Bij het bewaken en beveiligen van VIPS zijn de volgende organisaties betrokken: het ministerie van Binnenlandse Zaken, de UCLAT, verschillende Franse veiligheidsdiensten, de nationale politie, specifiek de SDLP, *de Gendamerie* en de *Garde Républicaine.*

Voor het inschatten van dreigingen zijn de veiligheidsdiensten en andere onderdelen van de nationale politie betrokken. Als er sprake is van terrorismedreiging, dan is het coördinerende orgaan de UCLAT betrokken. Het ministerie van Binnenlandse zaken gaat de toewijzing van (aanvullende) maatregelen voor VIPS. Alle VIPS worden beveiligd door de verschillende eenheden van de SDLP.[167] Tijdens bijvoorbeeld ceremonies wordt de beveiliging ondersteund door een eenheid van de Gendarmerie nationale, genaamd *de Garde Républicaine*.[168]

6.4.11 (Kroon)getuigen

Frankrijk heeft geen formeel getuigenbeschermingsprogramma. De Gendamerie is betrokken bij individuen die vanwege hun betrokkenheid bij een strafzaak onder dreiging staan. Onder het ministère de l'intérieure is de *Commission nationale de protection et réinsertion opgericht*[169] om uitvoer te geven aan de beschermingsregels van kroongetuigen die vastgelegd zijn in de Code de procédure pénale.[170]

6.5 Italië

6.5.1 Inleiding

Dreigingen voor personen komen in Italië in belangrijke mate uit de hoek van de georganiseerde misdaad, waarbij deze vorm van misdaad zich vooral richt op medewerkers van het Openbaar Ministerie en rechters, en in mindere mate op politici. Voornamelijk politici waren tot twee decennia geleden doelwit van terrorisme.[171] Het stelsel van bewaken en beveiligen is in 2002 herzien na de moord door de nieuwe Rode Brigade op Marco Biagi, jurist, econoom en politiek adviseur, wiens persoonlijke beveiliging enkele maanden daarvoor was stopgezet. In 2014 werden zo'n 600 personen

[165] Arrêté du 19 octobre 1994 portant organisation à la direction générale de la police nationale du service de protection des hautes personnalités, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000164562/.
[166] Art. 5 Arrêté du 12 août 2013 relatif aux missions et à l'organisation du service de la protection.
[167] Arrêté du 17 décembre 2008 relatif aux missions et à l'organisation du service de protection des hautes personnalités; Arrêté du 12 août 2013 relatif aux missions et à l'organisation du service de la protection.
[168] https://www.gendarmerie.interieur.gouv.fr/garde-republicaine/.
[169] Zie: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028745334/.
[170] Articles 706-57 – 706-63 Code de procédure pénale.
[171] Bakker & Vos 2023, p 8.

beveiligd binnen het stelsel, waaronder bijvoorbeeld journalisten, ondernemers en topambtenaren.[172] Ongeveer een derde daarvan bevond zich in Rome. Het aantal beveiligde personen was vele male hoger dan in andere Europese hoofdsteden, zoals Londen (43 beveiligde personen) en Parijs (41).[173] Anno 2025 ontvangen nog steeds ongeveer 600 personen beveiliging.[174]

In de Italiaanse cultuur accepteren personen die worden beveiligd over het algemeen de beveiligingsmaatregelen makkelijker, omdat zij weten dat het bij het ambt hoort, en zijn daardoor mentaal weerbaar ten opzichte van de uitdagingen die bij persoonsbeveiliging komen kijken.[175] In Italië bestaan wel twijfels over de grootte van de lijsten met te beveiligen personen vanwege het feit dat het hebben van beveiliging kan worden gezien als een “statussymbool”.[176]

Verder treden te beveiligen personen opvallend vaak naar buiten met naam en gezicht op bijvoorbeeld social media, in tegenstelling tot andere landen.[177] Volgens Italiaanse magistraten is de logica daarachter dat bekendheid geven aan het feit dat je als individu wordt bedreigd, tevens een persoon kan beschermen.[178]

De beveiliging van personen kan in Italië worden ingezet wanneer er sprake is van een gevaar of bedreiging (zowel potentieel als feitelijk). De bedreigingen moeten van terroristische aard zijn of verband houden met georganiseerde misdaad, handel in verdovende middelen, wapens of bijvoorbeeld nucleair, radioactief materiaal en chemische en biologische agentia, of in verband kunnen worden gebracht met inlichtingenactiviteiten van buitenlandse entiteiten of organisaties. Het gaat onder andere om personen die vanwege hun publieke optreden en opinies bedreigd worden, denk aan journalisten en activisten, maar ook bijvoorbeeld advocaten, rechters of (hoge) ambtenaren.

6.5.2 Rolverdeling en verhouding tussen betrokken organisaties

Het stelsel van bewaken en beveiligen wordt in Italië georganiseerd door verschillende overheidsinstanties, waarbij een onderscheid wordt gemaakt tussen nationale en lokale veiligheidsdiensten. Er is geen sprake van een publiek-private samenwerking.[179]

De centrale verantwoordelijkheid voor de bescherming van personen in Italië ligt bij het ministerie van Binnenlandse Zaken en meer specifiek de UCIS, die verantwoordelijk is voor de beveiliging van deze categorie personen.[180] De UCIS beoordeelt risicoanalyses, onderzoekt specifieke situaties waarin sprake is van dreigingen, evalueert deze en neemt passende maatregelen.

---

[172] https://www.agi.it/fact-checking/news/2018-06-23/persone_sotto_scorta_italia-4059868/. In dit getal is niet de bescherming van (kroon)getuigen en hun families opgenomen.
[173] Cijfers uit 2014; Italia dei Valori 2014.
[174] Onder dit getal vallen niet de beschermde kroongetuigen.
[175] Bakker & Vos 2023, p 19.
[176] https://magazines.openbaarministerie.nl/opportuun/2022/04/italiaanse-mafia-aanpak-als-leerschool; Italia dei Valori 2014; https://www.asaps.it/39007-_agenti_di_scorta__uno__status_symbol_.html; Zie ook dit voorbeeld waarin een minister in opspraak kwam nadat haar beveiliging haar kar in de IKEA moest duwen: https://www.corriere.it/politica/12_maggio_24/finocchiaro-all-ikea-con-scorta_91fb9552-a570-11e1-8ebb-5d15128b15be.shtml.
[177] https://magazines.openbaarministerie.nl/opportuun/2022/04/italiaanse-mafia-aanpak-als-leerschool; Bakker & Vos 2023, p 8.
[178] Idem.
[179] Bakker & Vos 2023, p 24.
[180] https://www.interno.gov.it/it/ministero/dipartimenti/dipartimento-pubblica-sicurezza.

De prefect speelt een sleutelrol in het stelsel. Wanneer er sprake is van een dreigende situatie verzamelt de prefect op lokaal ('periferisch') niveau informatie en rapporteert deze informatie aan de UCIS. Na akkoord zet de prefectuur de opdracht uit bij een van de hierna genoemde (politie)diensten.

De Polizia di Stato is verantwoordelijk voor de algemene handhaving van de wet op nationaal niveau, inclusief de bescherming van personen (zo'n 40% van alle gevallen). De Carabinieri (ook zo'n 40% van alle gevallen) vervult ook binnenlandse veiligheidsfuncties. Beide diensten hebben in de praktijk vergelijkbare taken en functies die elkaar afwisselen. De Guardia di Finanza richt zich voornamelijk op economische criminaliteit, maar kan ook worden ingezet voor de bescherming van personen, wanneer het om bedreigingen vanuit de georganiseerde misdaad gaat (zo'n 20% van alle gevallen). De hiervoor genoemde diensten werken ook samen binnen dezelfde beveiligingsopdrachten.

Ten slotte hebben de veiligheidsdiensten, waaronder de AISI voor binnenlandse inlichtingen, de AISE voor externe inlichtingen, het veiligheidsdepartement DIS en regionale diensten een rol in het aanleveren van dreigingsinformatie aan de UCIS, met name op het gebied van terroristische dreigingen.

6.5.3 Aanleiding inzet van het stelsel

De inzet van het stelsel kan in Italië verschillende aanleidingen hebben. Zo kan een aangifte de aanleiding zijn om het stelsel te activeren of de aanwezigheid van bepaalde, andere dreigingsinformatie bij de lokale politie.

6.5.4 (Dwang)bevoegdheden voor informatieverzameling en dreigingsanalyses

In Italië is het proces van informatieverzameling en het opstellen van dreigingsanalyse vanuit de dreigingen van terrorisme en de georganiseerde misdaad nagenoeg hetzelfde.[181] Daarom zijn deze samengenomen. De inlichtingendiensten leveren met name in geval van terrorisme informatie bij de UCIS aan (zie hierna), en hebben in het kader van de veiligheid van de Staat bevoegdheden om inlichtingen te verzamelen. In het kader van terrorismebestrijding hebben de inlichtingendiensten de dwangbevoegdheid om communicatie af te luisteren. Hiervoor is wel toestemming vereist van de Procureur-generaal van het Hof van Beroep van Rome.[182] Bij beide type dreigingen is het echter de politie die het voortouw neemt wat betreft het opstellen van een dreigingsanalyse.

De betrokken lokale politiedienst verzamelt in de eerste plaats de relevante informatie. Voor het verzamelen van informatie bestaan geen aparte dwangbevoegdheden in het kader van bewaken en beveiligen. Het is niet mogelijk om een apart politieonderzoek te starten om de waardering van de dreiging in een bepaalde situatie in te kunnen schatten. Er kan wel gebruik worden gemaakt van open bronnen, politie-informatie en strafrechtelijke onderzoeken die al lopend of afgerond zijn.

Om te bepalen in welk niveau een te beschermen persoon ingeschaald moet worden, geeft de wet de volgende parameters:

[181] Zie art. 1 DECRETO-LEGGE 6 maggio 2002, n. 83, waarin terrorisme en georganiseerde misdaad beiden worden genoemd als mogelijke oorzaken van gevaren of bedreigingen tegen personen.
[182] Art. 4 DECRETO-LEGGE 27 luglio 2005, n. 144.

- de functie die de te beschermen persoon bekleedt, mede gelet op vroegere functies en activiteiten;
- de bekendheid die is verworven via de massamedia of in de eigen werkomgeving;
- de omgevingscontext waarin het gevaar en de dreiging zijn ontstaan;
- de analyse van de dreiging met betrekking tot het soort criminele organisatie waarvan deze uitgaat;
- de aanwezigheid van deze organisatie op het grondgebied en of deze zich naar andere provincies of regio's heeft uitgebreid;
- de relatie tussen de organisatie en de bedreigde persoon;
- de wijze waarop de situaties van gevaar of bedreiging zich hebben gemanifesteerd;
- het soort bedreiging;
- de geloofwaardigheid van de dreiging in verhouding tot de criminele capaciteit van de organisatie waarvan zij uitgaat;
- alle andere subjectieve en objectieve informatie waaruit het bestaan van een risicosituatie kan worden afgeleid;

Er wordt gebruik gemaakt van verschillende soorten dreigingsniveaus (van 1 tot en met 4, waarbij niveau 1 het hoogste is) ter invulling van de Legge 133/2002.[183] Voor alle niet-VIPS wordt een persoonlijke, informatiegestuurde afweging van de dreiging gemaakt. De prefect maakt, samen met de lokale politiediensten, een inschatting welk dreigingsniveau van toepassing is en stelt maatregelen voor aan UCIS. De situatie wordt in een technisch overleg besproken.

De niveaus luiden als volgt:[184]

- Primo livello (eerste niveau, exceptioneel risico): er is sprake van een acuut, evident en zeer verhoogd risico. Per situatie moet bekeken worden welke 'exceptionele beveiliging' noodzakelijk is;
- Seconde livello (tweede niveau, zeer hoog risico): er is sprake van reële en actuele dreiging of gevaar, direct of indirect. De beveiliging bestaat uit pantserwagens met drie bewakers in burgerkleding. Deze maatregelen kunnen worden aangevuld met extra beveiliging bij woning en/of werkplaats.
- Terzo livello (derde niveau, hoog risico): de te beveiligen persoon loopt het risico om doel te worden van criminele activiteiten en/of aanslagen. De beveiliging bestaat uit één gespecialiseerde auto met een gewapende escorte (of twee indien de situatie hierom vraagt). Ook hierbij geldt dat extra maatregelen bij woning en/of werkplaats kunnen ingezet, afhankelijk van de situatie.
- Quarto livello (vierde niveau, medium risico): In dit geval is het gevaar nog onvoldoende vastgesteld en actueel. De beveiliging bestaat uit een niet-beveiligde auto met één bewapende escorte.

[183] https://www.concorsipolizia.it/scorta-di-sicurezza/.
[184] Decreto del Ministero Dell'interno 28 maggio 2003, n. 557/A/208.018.IS.79.

6.5.5 Het delen van informatie tussen betrokken partijen

De UCIS heeft een sleutelrol in de coördinatie van de bewaking en beveiliging en in de te nemen maatregelen. Voor deze taak ontvangt UCIS informatie van zowel de politie als de inlichtingendiensten, met name in geval van een terroristische dreiging. De meeste informatie wordt mondeling uitgewisseld, door het bijeenroepen van de hiervoor genoemde technische overleggen. Snelheid is geborgd doordat het mogelijk is om een dergelijke bijeenkomst spoedig bijeen te roepen.

In het decreto-legge 6 maggio 2002 wordt benoemd van welke informatiebronnen de UCIS gebruik kan maken en onder welke voorwaarden die informatie van bijvoorbeeld de veiligheidsdiensten kan worden verkregen. Er is geen materiewetgeving aangetroffen waarin de verstrekking van persoonsgegevens ten behoeve van het bewaken en beveiligen van personen expliciet is gereguleerd. De UCIS doet zelf geen onderzoek en kan niet direct databases raadplegen. Daarvoor moet een informatieverzoek worden ingediend bij de politie. Op basis van een informatieverzoek deelt de politie enkel de noodzakelijke informatie met de UCIS (vergelijkbaar met een hit/no-hit systeem). Dat is in de regel niet de onderliggende brondocumentatie.

De UCIS kan tevens de rechtbank verzoeken om informatie te ontvangen over strafrechtelijke handelingen. Dit gebeurt met tussenkomst van de minister van Binnenlandse Zaken.[185] Gegevens over strafrechtelijke handelingen worden in een register opgeslagen waartoe een rechterlijke instantie toegang kan verlenen. Ook kan de rechtbank op eigen initiatief afschriften en informatie toezenden aan speciaal daarvoor gemachtigde ambtenaren. De UCIS kan dus in samenwerking met andere instanties informatie verzamelen die onder andere zien op justitiële en strafvorderlijke feiten in een bepaalde casus.[186] Informatie over beveiligingsmaatregelen wordt als geclassificeerd bestempeld. Slechts een beperkte groep die aan specifieke vereisten voldoet heeft toegang tot deze informatie.

6.5.6 Het nemen en uitvoeren van maatregelen

De UCIS oordeelt over voorstellen, wijzigingen, verlenging of afschaffing van maatregelen. De prefect kiest uit een van de vier ‘standaard’ beveiligingsniveaus, maar kan ook voorstellen dat een van de niveaus wordt aangevuld met aanvullende maatregelen of over gaan tot losse maatregelen (zonder link met een van de vier standaardpakketten). De UCIS beoordeelt de situatie en bepaalt de definitieve beveiligingsmaatregelen. Hierbij kan informatie uit andere prefecturen of centrale directoraten gebruikt worden. Na akkoord zet de prefectuur de opdracht uit bij een van de (politie)diensten.

De maatregelen worden vervolgens decentraal uitgevoerd. De prefect kan zelfstandig voorzien in aanvullende maatregelen indien nodig. Deze bewakingsmaatregelen worden uitgevoerd door lokale politiediensten, met name de Polizia de Stato, de Carabinieri en de Guardia Finanza, en kunnen onder andere bestaan uit dynamische en statische bewaking, bewaking op bepaalde tijdstippen en generieke radio verbonden bewaking.

Te beveiligen personen tekenen een overeenkomst waarin zij akkoord gaan met de maatregelen en het uitgangspunt dat het openbare belang prevaleert boven het particuliere belang van de persoon.

---

[185] Decreto del Presidente della Repubblica 22 settembre 1988, n. 447 (artikel 118) en Decreto-legge 6 maggio 2002, n. 83 (artikel 2 lid 4).
[186] Idem.

Personen gaan er dus mee akkoord dat de maatregelen inbreuk kunnen maken op hun persoonlijke levenssfeer om gepaste beveiliging mogelijk te maken. Er zijn vergaande plichten opgenomen waar de persoon zich aan dient te houden (zoals het melden van de activiteiten die iemand doet of voornemens is, de plicht om niemand te vertellen waar die persoon heen gaat). Gaat de persoon niet akkoord, dan krijgt hij geen beveiliging.

Het gaat om een standaardcontract dat voor alle te bewaken personen hetzelfde is. Hierin is dus geen ruimte voor maatwerk.

6.5.7 Het evalueren/bijstellen van dreigingsanalyses/maatregelen

De dreigingsinschatting wordt afhankelijk van de situatie elke drie of zes maanden herzien in technische coördinatie overleggen, voorgezeten door de prefect van het betreffende gebied, waarbij hoofden van politiediensten op provinciaal niveau en de UCIS aanwezig zijn. Deze technische overleggen vinden plaats wanneer dat noodzakelijk wordt geacht. Naast het feit dat de evaluatie elke drie of zes maanden plaatsvindt, is er wel sprake van continue monitoring om het actuele risico in de gaten te houden.

6.5.8 Het afbouwen van maatregelen

De UCIS is ook verantwoordelijk voor het nemen van de beslissingen over het afbouwen van maatregelen. Maatregelen worden alleen geleidelijk afgebouwd en pas ingetrokken wanneer is vastgesteld dat er geen sprake meer is van een dreiging. Bij twijfel of wanneer meer informatie nodig is, kan de UCIS een adviescomité bij elkaar roepen met politie- en geheime diensten en de prefect als voorzitter.

6.5.9 Toezicht op het stelsel

Er is in Italië geen sprake van een toezichthoudende instantie. Het toezicht is belegd ‘in de lijn’ en de minister van Binnenlandse Zaken is eindverantwoordelijk. Er vinden wel overleggen plaats, bijvoorbeeld via het Parlementaire Comité voor de Veiligheid van de Republiek (COPASIR), maar er bestaat geen toezichthouder op het stelsel.

6.5.10 VIPS

In Italië is de bescherming van belangrijke personen (VIPS) onder meer geregeld in wetten zoals de legge 121 van 1981 en de wijziging uit 2002 die de bescherming van belangrijke personen, zoals politici, rechters en diplomaten, waarborgen. De decreto-leggo 6 maggio 2002, n.83 regelt de bescherming van onder meer Italiaanse regeringsfunctionarissen en hoge institutionele functionarissen, buitenlandse hooggeplaatste personen en personen die uit hoofde van hun functie risico lopen.[187]

Er bestaat een lijst met zestien categorieën van functies die onder het eerste (het zwaarste) dreigingsniveau vallen.[188] Het gaat om de volgende functies: de huidige en voormalige presidenten van de republiek van Italië, de premier, de vicepremier, president van de Italiaanse senaat, voorzitter van de kamer der afgevaardigden, voorzitter van het Grondwettelijke Hof, minister van Binnenlandse

[187] Zie Decreto-legge 6 maggio 2002, n. 83.
[188] Decreto del Ministero Dell’interno 28 maggio 2003, n. 557/A/208.018.IS.79.

Zaken, minister van Defensie, minister van Justitie, minister van Buitenlandse Zaken, minister van Economie en Financiën, Onderstaatssecretaris van het voorzitterschap van de Raad van Ministers, eerste voorzitter en procureur-generaal van het Hof van Cassatie en de vicevoorzitter van de Hoge Raad voor Justitie. Deze personen worden op basis van hun functie het zwaarste beveiligd, ongeacht de dreiging.

De centrale verantwoordelijkheid voor de bescherming VIPS ligt bij het ministerie van Binnenlandse Zaken. De beveiliging van VIPS wordt uitgevoerd door de Polizia di Stato en de Caribinieri (militaire politie die valt onder de verantwoordelijkheid van het ministerie van Defensie).

De veiligheidsdiensten, waaronder de AISI voor binnenlandse inlichtingen, de AISE voor externe inlichtingen, het veiligheidsdepartement DIS en regionale diensten hebben een rol in het aanleveren van dreigingsinformatie, met name op het gebied van terroristische dreigingen.

6.5.11 (Kroon)getuigen

De Legge del 6 febbraio 1980 n. 15, de Decreto-legge 15 gennaio 1991, n. 8 en de Legge 13 febbraio 2001 bevatten nadere regels over 'samenwerking met justitie' (spijtoptanten, of in het Italiaans: collaboratori di giustizia) en getuigen. De Italiaanse wetgeving maakt een onderscheid tussen getuigen met en zonder criminele achtergrond. Binnen die laatste categorie vallen bijvoorbeeld criminelen die eerst lid waren van een criminele organisatie, en nu informatie verschaffen aan justitie. De Legge n. 6 del 2018 (sui testimoni di giustizia) verduidelijkt het onderscheid tussen deze categorieën getuigen. Een verzoek tot bescherming kan worden ingediend door de officier van justitie. Een commissie, bestaande uit personen met specifieke ervaring in het veiligheidsdomein, beslist over de toelating tot het beschermingsprogramma en de maatregelen die hieruit voortvloeien. Het betreft een ondersecretaris van het ministerie van Binnenlandse Zaken, twee officieren van justitie, een advocaat van de staat en vijf ambtenaren. Zij beslissen met een meerderheid van stemmen. De 'collaboratori di giustizia' en getuigen worden beschermd door de Servizio centrale di protezione, een andere beschermingseenheid dan de UCIS. In 2022 werden 892 kroongetuigen beveiligd.[189] Het ministerie van Binnenlandse zaken speelt een belangrijke rol bij het voeren van de administratieve rechtsgang rondom kroongetuigen, het Openbaar Ministerie beoordeelt slechts de verklaring en adviseert over het belang en het risico van de getuige.

Voor kroongetuigen geldt dat de wet onderscheid maakt tussen reguliere en bijzondere beschermingsmaatregelen, en een bijzonder beschermingsprogramma.[190] Politiediensten passen de reguliere beschermingsmaatregelen toe. Deze kunnen aangevuld worden met bijzondere maatregelen indien blijkt dat de reguliere bescherming onvoldoende is. De zwaarste beveiliging wordt toegepast op kroongetuigen die onder het beschermingsprogramma vallen. De kroongetuige en zijn familie wordt in dat scenario overgeplaatst naar een beschermde locatie in andere regio.

[189] Peters 2023. Via https://repository.wodc.nl/bitstream/handle/20.500.12832/3270/3370-hoofdlijnen-bestrijding-maffiacriminaliteit-italie-volledige%20tekst.pdf.
[190] Peters 2023. Via https://repository.wodc.nl/bitstream/handle/20.500.12832/3270/3370-hoofdlijnen-bestrijding-maffiacriminaliteit-italie-volledige%20tekst.pdf.

In 2018 trad een nieuwe wet in werking om getuigen te beschermen, de Legge 11 gennaio 2018, n. 6. Deze wet moet zorgen voor verbeterde maatregelen die de positie van getuigen versterken, waaronder economische, sociale en financiële ondersteuning.

6.6 Spanje

6.6.1 Inleiding

Spanje kent een lange geschiedenis van terrorismebestrijding in verband met de Baskische afscheidingsbeweging ETA.[191] Dit is mogelijk de aanleiding geweest om tot een robuust en ontwikkeld systeem van persoonsbeveiliging voor politici, rechters, andere overheidsfunctionarissen en journalisten te komen. Daarnaast vormt Spanje net als Nederland een belangrijke schakel in de internationale drugshandel, met soortgelijke strafrechtzaken zoals die in Nederland worden gevoerd. Net als in Nederland is persoonsbeveiliging zeer waarschijnlijk aan de orde in dergelijke situaties.

De Constitución Española (1978) regelt in artikel 17 het recht op vrijheid en veiligheid. Dit recht wordt in verschillende wetten op verschillende terreinen uitgewerkt, zoals de Wet op Terrorismebestrijding (Ley Orgánica 2/2002, de Protección de las Víctimas del Terrorismo), Wet op de Getuigenbescherming (Ley de Protección de Testigos y Peritos en Causas Criminales, 19/1994)[192]), de Wet op de Strafrechtspleging (Ley de Enjuiciamiento Criminal) en het Spaanse Wetboek van Strafrecht (Código Penal). Het recht op vrijheid en veiligheid brengt met zich mee dat in sommige gevallen persoonsbeveiliging noodzakelijk wordt geacht voor personen die niet op basis van hun functie automatisch worden beveiligd.

6.6.2 Rolverdeling en verhouding tussen betrokken organisaties

Het *Ministerio del Interior* speelt een centrale rol in de coördinatie van het stelsel van bewaken en beveiligen. Onder dit ministerie valt *la Secretaria de Estado de Seguridad* (het Staatssecretariaat voor Veiligheid). Het *Ministerio del Interior* beschikt over een eigen inlichtingendienst, de *Centro de Inteligencia contra el Terorrisme y el Crimen Organizado* (CITCO), wat zich voornamelijk bezighoudt met inlichtingen die specifiek zien op terrorisme en georganiseerde misdaad.[193] CITCO is een samenvoeging van het voormalige Inlichtingencentrum tegen Georganiseerde Misdaad (CICO) en het Nationaal Coördinatiecentrum voor Terrorismebestrijding (CNCA).[194]

La Secretaria de Estado de Seguridad voert verschillende taken uit in het kader van veiligheid. Zo coördineert het Staatssecretariaat de (internationale (politie))diensten en houdt zij toezicht op hen en

[191] Zie voor meer informatie: https://www.lamoncloa.gob.es/lang/en/espana/stpv/spaintoday2015/security/Paginas/index.aspx. Spanje en Frankrijk werken ook samen in de strijd tegen terrorisme.
[192] https://ocindex.net/2021/country/spain. Deze wet bestaat uit slechts vier artikelen en biedt onvoldoende waarborgen om een getuige daadwerkelijk te beschermen, vinden critici.
[193] https://www.interior.gob.es/opencms/es/detalle/articulo/El-secretario-de-Estado-de-Seguridad-ensalza-la-trayectoria-del-CITCO-en-la-identificacion-y-neutralizacion-de-las-amenazas-del-terrorismo-y-el-crimen-organizado/.
[194] Real Decreto 873/2014, de 10 de octubre, por el que se modifica el Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. Meer wetgeving over anti-terrorisme is geregeld in de Ley Orgánica 2/2002, de Protección de las Víctimas del Terrorismo.

de missies die zij uitvoeren.[195] Ook coördineert, leidt en bevordert zij acties tegen zware criminaliteit waaronder georganiseerde misdaad en terrorisme.

Het *Centro Nacional de Inteligencia* (CNI) valt onder het *Ministerio de Defense* (Defensie) en is de Spaanse Geheime Dienst.

Het *Ministerio de Justicia* (vergelijkbaar met het Nederlandse ministerie Justitie en Veiligheid) is in mindere mate betrokken. Het ministerie houdt zich onder andere bezig met wetgeving[196], rechtspraak en penitentiaire instellingen[197] (in een gedeelde verantwoordelijkheid met BZK)[198], en daardoor minder met openbare orde en veiligheid. In Spanje is BZK hier primair verantwoordelijk voor.

De Spaanse Minister-President wordt geadviseerd over veiligheidskwesties door *el Departamento de Seguridad Nacional* (Departement van Nationale Veiligheid). Het departement beschikt over gespecialiseerde comités op het gebied van terrorisme en georganiseerde misdaad.[199] Als taken heeft zij onder andere het uitvoeren van onderzoek, het ontwikkelen en implementeren van strategieën, coördinatie en het monitoren van nationale en internationale risico's.[200] *La Secretaría de Estado de Seguridad* is verantwoordelijk voor de bescherming van mensenrechten, met name die van persoonlijke vrijheid en beveiliging.[201] Zij kan bevel aan *las Fuerzas y Cuerpos de Seguridad* geven, hun missies coördineren en toezicht houden. Las Fuerzas y Cuerpos de Seguridad omvatten de nationale regionale en lokale politiediensten.[202]

In Spanje zijn er verschillende politiediensten die zich inzetten voor de bewaking en beveiliging van personen, gebouwen en faciliteiten. Voor wat betreft de politiediensten zijn op landelijk niveau betrokken: de *Policía Nacional* (de Nationale politie) en de *Guardia Civil* (het Spaanse equivalent van de Koninklijke Marechausee). Op gemeentelijk niveau bestaan er nog verschillende korpsen (*Policía Local*). Deze politiediensten vallen alle drie onder het *Ministerio del Interior.* Daarnaast bestaan er autonome politiekorpsen zoals de Mossos d'Esquadra (voor Catalonië) en Ertzaintra (voor het Baskenland).

In Spanje wordt gebruik gemaakt van zowel publieke als private beveiliging. De Staat is verantwoordelijk voor het waarborgen van openbare veiligheid, en de overheid voor beveiliging.[203] Spanje ziet echter mogelijkheden in publiek-private samenwerkingen om de mate van veiligheid en beveiliging verder te verhogen[204] en heeft hiervoor ook een samenwerkingsverband opgericht.[205] Zo is

---

[195] https://www.interior.gob.es/opencms/es/el-ministerio/funciones-y-estructura/secretaria-de-estado-de-seguridad/
[196] https://www.mpr.gob.es/mpr/funciones/Paginas/funciones.aspx.
[197] Articulo setenta y nueve, Ley Orgánica 1/1979 de General Penitenciaria (https://www.boe.es/buscar/act.php?id=BOE-A-1979-23708).
[198] https://www.prison-insider.com/en/countryprofile/espagne-2018?s=vue-d-ensemble#vue-d-ensemble; Ocaña 2013. Via https://www.prisonobservatory.org/upload/PrisonconditionsinSpain.pdf.
[199] https://www.dsn.gob.es/en/node/7.
[200] Real Decreto 1119/2012, de 20 de julio, de modificación del Real Decreto 83/2012, de 13 de enero, por el que se reestructura la Presidencia del Gobierno.
[201] https://www.interior.gob.es/opencms/es/el-ministerio/funciones-y-estructura/secretaria-de-estado-de-seguridad/.
[202] Ley Orgánica de Fuerzas y Cuerpos de Seguridad, 2/1986.
[203] Articulo 149.1.29 Spanish Consitution; Articulo uno Ley Orgánica 2/1986 de Fuerzas y Cuerpos de Seguridad.
[204] Ley 5/2014 de Seguridad Privada.
[205] https://www.policia.es/_es/tupolicia_red_azul.php.

het mogelijk om zelf een verzoek in te dienen voor particuliere beveiliging.[206] Dit houdt in dat personen een gemotiveerde brief sturen aan la Unidad Central de Seguridad Privada (de centrale eenheid van particuliere beveiliging) of een van de Unidades Provinciales (provinciale eenheden) waarin ze de redenen aangeven waarom beveiliging in een gegeven situatie noodzakelijk is.

6.6.3 Aanleiding inzet van het stelsel

Er is geen informatie bekend over de aanleiding om het stelsel in te zetten voor bedreigde personen in Spanje.

6.6.4 (Dwang)bevoegdheden voor informatieverzameling en dreigingsanalyses

De Ley Orgánica 7/2021, de implementatiewet van de Europese richtlijn gegevensbescherming politie en justitie, heeft als doel om personen te beschermen wanneer hun gegevens worden verwerkt met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten of de uitvoering van strafrechtelijke sancties. Daar valt ook de bescherming en preventie van bedreigingen voor de openbare veiligheid onder. De wet is van toepassing op zowel geautomatiseerde als niet-geautomatiseerde verwerkingen behoudens uitzonderingen en legt rechten en plichten op het gebeid van gegevensbescherming vast. De bevoegde autoriteiten die volgens de wet belast zijn met voorkomen, opsporen, onderzoeken, vervolgen, bescherming en preventie, worden tevens gezien als bevoegde autoriteiten om gegevens te verwerken. Verwerking mag alleen voor deze doeleinden plaatsvinden. Er bestaat een plicht tot samenwerking waarbij gegevens – voor zover noodzakelijk – worden gedeeld om taken naar behoren uit te kunnen voeren.

In deze wet wordt onderscheid gemaakt tussen verschillende categorieën personen op wie deze regels van toepassing kunnen zijn; er wordt dus bijvoorbeeld onderscheid gemaakt tussen personen die veroordeeld zijn voor een strafbaar feit en derden zoals getuigen. In deel twee van de wet licht de wetgever specifiek verschillende soorten verwerkingen toe op het gebied van videobewaking.

Het CITCO ontvangt en analyseert voortdurend informatie, waarmee periodieke dreigingsbeelden worden gemaakt.[207] Deze beelden helpen met het formuleren en coördineren van een nationale aanpak en de (operationele) coördinatie tussen verschillende diensten, en waar noodzakelijk, welke acties zij moeten ondernemen.[208] Ook brengt het CITCO jaarverslagen uit en bepaalt de strategie voor de aanpak van terrorisme en georganiseerde misdaad in Spanje en coördineert en controleert de uitvoering daarvan.[209]

Het CNI opereert algemener dan het CITCO en ziet op nationale veiligheid in de brede zin. Het CNI is verantwoordelijk voor het verstrekken van informatie, analyses, studies of voorstellen aan de

---

[206] https://sede.policia.gob.es/portalCiudadano/_en/tramites_seguridadprivada_tramite_vigilantesdeseguridadconarmas.php.

[207] https://www.lamoncloa.gob.es/lang/en/espana/stpv/spaintoday2015/security/Paginas/index.aspx.

[208] Articulo dos sub c, Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. https://www.boe.es/buscar/act.php?id=BOE-A-2018-10755.

[209] Articulo dos sub c-3, Real Decreto 952/2018, de 27 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. https://www.boe.es/buscar/act.php?id=BOE-A-2018-10755. Punt 5 bepaalt dat het CITCO binnen het kader van haar bevoegdheden nationale strategieën voorstelt en deze bijwerkt, waarbij de ontwikkeling en uitvoering ervan worden gecoördineerd en gecontroleerd.

president en de regering over gevaar, dreigingen of agressie tegen de onafhankelijkheid van Spanje, haar nationale belangen en de stabiliteit van de rechtstaat.[210]

6.6.5 Het delen van informatie tussen betrokken partijen

Over het delen van informatie tussen betrokken partijen is geen informatie bekend, behalve dat er een plicht tot samenwerking bestaat waarbij gegevens – voor zover noodzakelijk – worden gedeeld om taken naar behoren uit te kunnen voeren (zie hiervoor).

6.6.6 Het nemen en uitvoeren van maatregelen

De *Policia Local* opereert in gemeenten met meer dan vijfduizend inwoners. Ze is daar belast met onder andere het voorkomen van criminele activiteiten, het bewaken van gebouwen en het samenwerken met andere politiediensten om de openbare ruimte te monitoren en beschermen (zoals bij grote menigtes).[211]

De *Policía Nacional* en de *Guardia Civil* opereren vaak landelijk en zijn direct ondergeschikt aan de centrale overheid. De *Policía Nacional* heeft jurisdictie in stedelijke gebieden. De *Guardia Civil* opereert vooral in landelijke gebieden en is betrokken bij de bescherming van kritieke infrastructuur, evenals grensbewaking en terrorismebestrijding.

De regionale politie-eenheden zoals de Mossos d'Esquadra en de Ertzaintza hebben hun eigen bevoegdheden binnen de autonome regio's, maar werken vaak samen met nationale eenheden in het geval van ernstige dreigingen. Hoe de exacte procedures zijn vormgegeven is niet duidelijk.

Over de plichten van de te bewaken persoon in Spanje is geen informatie bekend.

6.6.7 Het evalueren/bijstellen van dreigingsanalyses/maatregelen

Over het evalueren en bijstellen van dreigingsanalyses en maatregelen in Spanje is geen informatie bekend.

6.6.8 Het afbouwen van maatregelen

Over het afbouwen van maatregelen in Spanje is geen informatie bekend. Het is, net als in andere stelsels, onwaarschijnlijk dat de afbouw van maatregelen abrupt stopgezet kan worden. Doorgaans vindt afbouw plaats op basis van de actuele risicosituatie.

6.6.9 Toezicht op het stelsel

In Spanje vindt parlementaire controle op de inlichtingendiensten achteraf plaats. Het CNI verstrekt aan *el Congreso de los Diputados* (Congres van Afgevaardigden, onderdeel van het parlement) passende informatie over werking van de diensten en activiteiten.[212] De Presidente de la Cámara (voorzitter van het Huis) zit deze vergaderingen voor. De inhoud van deze vergaderingen is geheim. De commissie van het Congres die de kredieten van de inlichtingendienst controleert, heeft toegang tot gerubriceerde gegevens. Daar vallen bronnen en middelen van het CNI en buitenlandse diensten niet

[210] Articulo uno, Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.
[211] Artículo cincuenta y tres de Ley Orgánica 2/1984 de Fuerzas y Cuerpos de Segurdad.
[212] Articulo once Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

onder. De documenten worden bestudeerd door de commissie en vervolgens teruggegeven aan het CNI. De stukken, of kopieën daarvan, mogen niet worden bewaard.

De directeur van het CNI vraagt vooraf toestemming om maatregelen uit te oefenen waarbij het communicatiegeheim en de onschendbaarheid van woningen in het geding zijn.[213] Het verzoek wordt gedaan aan een magistraat van het Hooggerechtshof, alleen in dat geval dat het noodzakelijk is voor de taakuitvoering van het CNI.[214] Ten slotte is er politieke controle doordat de regering de directeur van het CNI benoemt en ontslaat en richtlijnen voor de inlichtingendienst samenstelt.[215]

6.6.10 VIPS

De leden van het Spaanse koningshuis en de minister-president worden op basis van de wet permanent beveiligd, ongeacht of een dreiging bestaat.[216] Het Spaanse Koninklijk huis wordt beveiligd door de *Servicio de Seguriad en de Guardia Real*. De *Servicio de Seguridad* valt onder het Secretariaat-Generaal van het Koninklijk huis. De Minister van Binnenlandse Zaken is eindverantwoordelijk, bepaalt de maatregelen en kan instructies geven aan de veiligheidsdienst.[217] Daarnaast bieden het ministerie van Binnenlandse zaken en Defensie, waaronder de *Guardia Civil*, ondersteuning waar dat nodig is.[218]

Voor de leden van het Koninklijk huis geldt dat standaard maatregelen niet worden afgebouwd. Hoewel dit niet uit de wet blijkt, is het aannemelijk dat aanvullende maatregelen worden afgebouwd zodra de dreiging niet meer actueel is.

De *Departamento de Seguridad is* verantwoordelijk voor de veiligheid van de minister-president en bepaalt de beveiligingsmaatregelen. Deze veiligheidsdienst is onderdeel van het Secretariaat-Generaal van de president en valt direct onder het gezag van de directeur van het Kabinet van de Premier. De veiligheidsdienst krijgt personeel van de *Fuerzas de Seguridad del Estado* (staatspolitie), toegewezen via het ministerie van Binnenlandse zaken.[219] Het ministerie van Binnenlandse Zaken biedt verder een ondersteunende rol. De *Departamento de Seguridad* is verantwoordelijk voor het verzamelen van informatie en het maken van dreigingsanalyses.[220] Net als bij het Koningshuis wordt informatieuitwisseling door de *Departamento de Seguridad* verondersteld, maar is onduidelijk om welke informatie het precies gaat en hoe de uitwisseling in de praktijk plaatsvindt.

Voor overige functies (denk aan leden van de regering, de vicepresident en dergelijke) geldt dat deze kunnen worden aangewezen door de directeur van het Kabinet van de Regeringsvoorzitter, in coördinatie met het *Ministerio del Interior* (de Spaanse equivalent van het ministerie van Binnenlandse Zaken).[221] Deze functies zijn aangewezen in een lijst.

Andere VIPS zoals ministers worden beveiligd door de nationale politie, met name door de *Unidad Central de Protección* (UCP) en de *Unidad de Intervención Policial* (UIP) die valt onder de *Comisaría*

---

[213] Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.
[214] Idem.
[215] https://www.cni.es/sobre-el-cni/organizacion .
[216] Real Decreto 434/1988, de 6 de mayo, sobre reestructuración de la Casa de S. M. el Rey; Art. 7 Real Decreto 890/2023, de 27 de noviembre, por el que se aprueba la estructura de la Presidencia del Gobierno.
[217] Art 7 Real Decreto 434/1988, de 6 de mayo, sobre reestructuración de la Casa de S. M. el Rey.
[218] Art 7 Real Decreto 434/1988, de 6 de mayo, sobre reestructuración de la Casa de S. M. el Rey.
[219] Art. 7 Real Decreto 890/2023, de 27 de noviembre, por el que se aprueba la estructura de la Presidencia del Gobierno.
[220] Art. 12 Real Decreto 890/2023, de 27 de noviembre, por el que se aprueba la estructura de la Presidencia del Gobierno.
[221] Art. 7 Real Decreto 890/2023, de 27 de noviembre, por el que se aprueba la estructura de la Presidencia del Gobierno.

General de Seguridad Ciudana. De verantwoordelijkheden van de Comisaría zijn vastgelegd in het Koninklijk Besluit 1334/1994 van 20 juni.[222] Onder de *Unidad* valt ook de *Brigada Central de Protecciones Especiales* die de beveiliging verzorgen van buitenlandse functionarissen of delegaties wanneer zij in Spanje verblijven.[223] Daarnaast is bepaald dat de *Guardia* ook buitenlandse staatshoofden zal beschermen indien dit bevolen wordt.[224]

6.6.11 (Kroon)getuigen

In Spanje wordt de bescherming van getuigen geregeld in de Wet op de Getuigenbescherming (Ley de Protección de Testigos y Peritos en Causas Criminales, 19/1994). Deze wet bestaat uit slechts vier artikelen. Om toegang te krijgen tot beschermingsmaatregelen moet een rechterlijke autoriteit oordelen of er sprake is van een ernstig gevaar voor een persoon. Ook echtgenoten of andere personen met wie deze persoon een affectieve relatie heeft, bloedverwanten in opgaande lijn, afstammelingen, broers en zussen kunnen beschermd worden. De rechter beoordeelt welke maatregelen in en bepaald geval noodzakelijk zijn. In uitzonderlijke gevallen kan een getuige voorzien worden van een nieuwe identiteit en financiële middelen om van woon- of werkplek te veranderen. Ook kunnen getuigen verzoeken om met dienstvoertuigen naar gerechtelijke gebouwen, de plek waar dep procedure wordt uitgevoerd, of naar hun woning te worden gebracht. Critici concluderen al meerdere jaren dat de wet onvoldoende waarborgen biedt om een getuige daadwerkelijk te beschermen.[225]

6.7 Verenigd Koninkrijk

6.7.1 Inleiding

Het Verenigd Koninkrijk heeft de afgelopen jaren meerdere terroristische aanslagen meegemaakt. In 2017 kwamen 22 personen om het leven en raakte 139 mensen gewond doordat een terrorist zichzelf opblies bij een concert in Manchester. Het was de meest dodelijke terroristische aanslag die het Verenigd Koninkrijk sinds 2005 had meegemaakt. Dat jaar werden wandelaars op de London Bridge en Westminster Bridge aangereden en een politieagent doodgestoken. Ook kreeg het land binnen vijf jaar tijd te maken met moorden op twee politici: Jo Cox (2016) en David Amess (2020). Na de dood van Cox groeide aandacht voor investering in het bewaken van beveiligen van personen en werd in vier maanden tijd vier keer zoveel geld aan beveiliging uitgegeven als in het hele jaar 2015.[226] Ook na de moord op Amess ontstonden vragen over de inzet van persoonlijke beveiligingsmaatregelen.[227]

De huidige terreurdreiging is ‘substantieel’.[228] Dat is niveau drie op een schaal van in totaal vijf niveaus.

---

[222] Zie artikel 15 lid 3 sub c.
[223] https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgseguridadciudadana_ucp.php.
[224] Articulo 6, Real Decreto 434/1988.
[225] Zie https://ocindex.net/2021/country/spain; https://ocindex.net/2023/country/spain. Waarom de bescherming ineffectief is gebleken, is niet duidelijk.
[226] https://www.dailymail.co.uk/news/article-3945430/MPs-spent-640-000-security-measures-four-months-killing-Jo-Cox-quadruple-figure-previous-year.html.
[227] https://news.sky.com/story/sir-david-amess-murder-mps-to-get-tailored-security-advice-after-killing-of-mp-southend-constituency-12601646.
[228] https://www.protectuk.police.uk/.

6.7.2 Rolverdeling en verhouding tussen betrokken organisaties

The Metropolitan Police Service (hierna: MPS) is de politiedienst van Groot-Londen (the Greater London Area). Naast het uitvoeren van de gebruikelijke politietaken in die regio, is de MPS ook verantwoordelijk voor terrorismebestrijding. De Protection Command is de afdeling die belast is met het bewaken en beveiligen en kent twee takken: de Royalty and Specialist Protection (hierna: RaSP) en de Parliamentary and Diplomatic Poretection (PaDP).

De RaSP is de verantwoordelijke dienst voor bescherming van leden van het koninklijk huis, ministers (inclusief de prime minister) bezoekende staatshoofden. De RaSP verzorgt ook de (gewapende) beveiliging van koninklijke residenties in Londen, Windsor en Schotland. De PaDP is daarnaast verantwoordelijk voor het bewaken van het parlementsgebouw en voor de bescherming van diplomatieke missies door het gehele Verenigd Koninkrijk.

De UKPPS biedt bescherming aan personen die het risico lopen om ernstige schade op te lopen, en de benodigde veiligheidsmaatregelen niet door de lokale politie of een daarvoor aangewezen dienst kunnen worden uitgevoerd.[229] Welke maatregelen getroffen worden is afhankelijk van het dreigingsniveau. De UKPPS geeft aan dat meestal een te beschermen persoon wordt verplaatst naar een andere locatie. Op regionaal niveau bestaan er ook Protected Persons Units, die samenwerken met de persoon die zich om veiligheidsredenen op een nieuwe woonplek vestigt. De verschillende diensten ondersteunen elkaar dus bij het beveiligen van personen.[230]

6.7.3 Aanleiding inzet van het stelsel

Er is geen informatie bekend over de aanleiding om het stelsel in te zetten voor niet-VIPS in het Verenigd Koninkrijk.

6.7.4 (Dwang)bevoegdheden voor informatieverzameling en dreigingsanalyse

In de Serious Organised Crime and Police Act 2005, hoofdstuk 4 is de ‘bescherming van getuigen en andere personen’ vastgelegd.[231] Het is aan degene die bescherming moet bieden om te bepalen welke maatregelen passend zijn bij het individuele geval. Daarbij moet rekening worden gehouden met het soort risico, de kosten van de maatregelen, hoe groot de kans is dat de te beschermen persoon zich kan aanpassen aan de maatregelen en hoe groot de kans is dat hij mogelijk een getuige is in een rechtszaak. De wet bepaalt dat de hoofdofficier van het politiekorps van Engeland en Wales, de hoofdcommissaris van de politiedienst in Schotland, de hoofdcommissaris van de politiedienst van Noord-Ierland, de directeur-generaal van de NCA, een commissaris voor ‘Her Majesty's Revenue and Customs’ of een persoon die door een van deze personen aangewezen is, bevoegd is om beschermingsmaatregelen te bepalen.

Daarnaast gelden nog verdragen als het EVRM (Human Rights Act), dat in artikel 2 *the right to life* vastlegt. Met betrekking tot de *threat to life*/*Osman warnings* is Osman/Verenigd Koninkrijk een belangrijk arrest van het EHRM. In dat arrest oordeelde het Hof uit artikel 2 van de Human Rights

[229] https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/providing-specialist-capabilities-for-law-enforcement/protected-persons.
[230] https://www.spa.police.uk/spa-media/taplt5o5/item-3-4-nca-performance-in-scotland.pdf.
[231] https://www.legislation.gov.uk/ukpga/2005/15/part/2/chapter/4.

Act/EVRM de positieve verplichting voor autoriteiten af om levensbedreigende situaties te voorkomen.

De Security Service Act 1989 regelt de oprichting van de binnenlandse veiligheidsdienst, de MI5. Deze act is in 1996 gewijzigd en aangevuld met meer informatie over de functie van de dienst en hun bevelen. De Intelligence Services Act 1994 betreft regels over de MI6, oftewel de buitenlandse inlichtingen.

Als het gaat om een *threat to life-warning* (ook wel O*sman-warning* genoemd; zie hoofdstuk 5) is de lokale politie de bevoegde organisatie. Dit zijn waarschuwingen van doodsbedreigingen vanuit politie en justitie, gericht aan het mogelijke slachtoffer. Wel geldt daarbij dat hoe hoger de dreigingsinschatting, hoe hoger deze in de lijn wordt uitgezet. Hoe de rolverdeling er precies uitziet bij welk niveau van dreiging verdient nader onderzoek.

6.7.5 Het delen van informatie tussen betrokken partijen

De Metropolitan Police Service deelt veel inlichtingen en data met andere organisaties.[232] Zo deelt zij informatie met de NCA, andere politiediensten, lokale autoriteiten en regionale units tegen georganiseerde misdaad. Door samen te werken is de service effectief gebleken in het in kaart brengen en tegengaan van deze dreigingen.

6.7.6 Het nemen en uitvoeren van maatregelen

Er is geen informatie bekend over hoe maatregelen worden genomen en uitgevoerd in het Verenigd Koninkrijk.

6.7.7 Het evalueren/bijstellen van dreigingsanalyses/maatregelen

Er is geen informatie bekend over hoe dreigingsanalyses en maatregelen worden geëvalueerd en bijgesteld in het Verenigd Koninkrijk.

6.7.8 Het afbouwen van maatregelen

Er is geen informatie bekend over hoe maatregelen worden afgebouwd in het Verenigd Koninkrijk.

6.7.9 Toezicht op het stelsel

Het Investigatory Powers Tribunal (IPT) is een onafhankelijk gerechtelijk orgaan dat klachten behandelt over misbruik van surveillance- en inlichtingenbevoegdheden door overheidsinstanties.[233] Ook behandelen ze klachten over de Britse inlichtingendiensten (de MI5, de MI6 en de Government Communications Headquarters (GHCQ). Het orgaan is opgericht middels sectie 65 van de Regulation of Investigatory Powers Act 2000 (RIPA). Deze wetgeving is inmiddels verouderd en vervangen door de Investigatory Powers Tribunal Rules 2018. De nieuwe regels zien onder andere toe op de verplichting dat klachtenbehandeling in het openbaar plaatsvindt (tenzij er zwaarwegende redenen zijn om dit niet

[232] HMICFRS 2019. Via https://assets-hmicfrs.justiceinspectorates.gov.uk/uploads/peel-assessment-2018-19-metropolitan.pdf.
[233] Home - The Investigatory Powers Tribunal.

te doen), het verstrekken van redenen wanneer klager in het ongelijk wordt gesteld, en het vastleggen van de rol van de 'counsel to the tribunal'.

Het IPT draagt daarnaast zorg voor het naleven van artikel 13 van het EVRM en klachten die voortkomen uit de Intelligence Service Act 1994.[234] De Tribunal staat in relatie tot de Investigatory Powers Commissioner, die hij om ondersteuning van het Tribunal kan verzoeken.[235] Information Commissioner's Office (ICO): Houdt toezicht op naleving van de UK GDPR en nationale privacywetgeving, inclusief gegevensdeling in beveiligingscontext.

Het Intelligence and Security Committee (ISC) is een parlementair comité dat toezicht houdt op de MI5, de MI6 en GCHQ, inclusief hun rol bij persoonsbeveiliging. Het comité is het eerste onderdeel van de Justice and Security Act 2013 geregeld. Dat is het VK-equivalent van de commissie in de Tweede Kamer die zich bezighoudt met de inlichtingen- en veiligheidsdiensten (Commissie-stiekem).

De commissie bestaat uit negen leden, afkomstig uit beide Huizen van het Parlement (House of Commons en House of Lords) en benoemd door het Parlement. De voorzitter van de commissie wordt gekozen door de leden van de commissie, op voordracht van de Prime Minister (in overleg met de oppositieleider).[236]

De commissie bepaalt haar eigen agenda en werkprogramma. Haar onderzoeken richten zich meestal op actuele gebeurtenissen en zorgwekkende kwesties en richten zich daarom op operationele en beleidskwesties, terwijl haar jaarverslagen ingaan op administratie en financiën. Bij het uitvoeren van haar onderzoeken stelt de commissie geen taakomschrijving vast, omdat het essentieel is dat de commissie het bewijs kan volgen en niet wordt beperkt in haar werkgebied.[237]

De commissie wordt bij haar werk ondersteund door het Office of The Intelligence and Security Committee. Dat is een klein team van analisten en onderzoekers (met inbegrip van juridische, technische en financiële expertise waar nodig). De bewijssessies worden besloten gehouden vanwege de gerubriceerde aard van het onderwerp en de commissie rapporteert jaarlijks aan de regering.[238]

[234] https://investigatorypowerstribunal.org.uk/about-the-tribunal/.
[235] Oversight and where we fit in - The Investigatory Powers Tribunal.
[236] Committee Membership – Intelligence and Security Committee of Parliament.
[237] How the Committee works – Intelligence and Security Committee of Parliament.
[238] Idem.

6.7.10 VIPS

De Protection Command is onderdeel van de MPS. Dit is de afdeling die belast is met het bewaken en beveiligen en kent twee takken; de Royalty and Specialist Protection (hierna: RaSP) en de Parliamentary and Diplomatic Protection (PaDP). De RaSP is de verantwoordelijke dienst voor bescherming van leden van het koninklijk huis, ministers (inclusief de prime minister) en bezoekende staatshoofden. De RaSP verzorgt ook de (gewapende) beveiliging van koninklijke residenties in Londen, Windsor en Schotland.

In het Verenigd Koninkrijk werken de politie en mentale gezondheidsinstellingen in het Fixated Threat Assessment Centre (FTAC) samen om een specifieke dreiging in beeld te brengen en te managen, namelijk die van de gefixeerde eenling. Het FTAC werd in 2006 opgericht en focust zich op personen met mentale problemen die publieke figuren bedreigen, zoals leden van de koninklijke familie, senior politici en locaties waar publieke figuren werken zoals Buckingham Palace. Politie en mentale gezondheidsinstellingen verzamelen informatie over de dreiging en voeren een dreigingsanalyse uit, om samen tot maatregelen te komen die patiënten en bedreigde personen ten goede komen. Het FTAC volgt richtlijnen die gelinkt zijn aan verschillende soorten risico's om te bepalen of zij een dreiging in behandeling nemen. Het gaat om uitzonderlijke situaties, zoals wanneer een verward persoon honderden brieven schrijft aan iemand of wanneer hij/zij denkt een romantische relatie te hebben met een publiek figuur.

239

6.7.11 (Kroon)getuigen

Het Verenigd Koninkrijk beschermt Britse (kroon)getuigen op basis van de Victims' Code of Practice, de Youth Justice and Criminal Evidence Act 1999 en het National Witness Protection Scheme. Er is geen specifieke wetgeving die zich richt op (kroon)getuigen. Het National Witness Protection Scheme werd in 2012 opgezet en biedt versterkte beveiliging aan getuigen die te maken hebben met een 'real and immediate' gevaar tegen hun leven.[240] Dit getuigenprogramma valt onder de National Crime Agency. De UKPPS is verantwoordelijk voor onder andere het versterken van lokale diensten, het verbeteren van het delen van inlichtingen tussen politiediensten en coördinatie van het systeem om bescherming van getuigen te kunnen garanderen.[241] Mogelijke beschermingsmaatregelen kunnen bestaan uit het anonimiseren van de getuige, het veranderen van zijn identiteit of het verhuizen naar een andere locatie.[242] Anonimisering speelt een rol in zaken met een hoog risico, waaronder georganiseerde misdaad en terrorisme.[243]

---

[239] https://hansard.parliament.uk/commons/2007-06-26/debates/0706279000039/FixatedThreatAssessmentCentre; James e.a. 2010. Via https://www.researchgate.net/publication/233475787_The_Fixated_Threat_Assessment_Centre_Preventing_harm_and_facilitating_care; https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(11)60113-X/fulltext.
[240] https://www.gov.uk/government/news/national-witness-protection-scheme-announced.
[241] https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/providing-specialist-capabilities-for-law-enforcement/protected-persons.
[242] https://www.cps.gov.uk/legal-guidance/witness-protection-and-anonymity.
[243] Hewathanthri 2024.

7. Landenvergelijking

7.1 Inleiding

In dit hoofdstuk vergelijken we de bevindingen in de onderzochte landen aan de hand van verschillende onderwerpen en antwoordmodaliteiten. Aan de hand van deze vergelijking is te zien waarin stelsels uniek zijn of juist overlap vertonen met andere landen. De vergaarde informatie per land is in dit hoofdstuk geplot in tabellen en in kolommen met antwoordmodaliteiten gesorteerd. Onder elk cluster van rijen wordt een toelichting gegeven bij de categorisering en worden opvallendheden benoemd. De tabellen en toelichtingen zijn een verdere uitwerking van onderzoeksvraag één tot en met drie en vijf. In een deel van de tabellen sluiten de verschillende antwoordmodaliteiten elkaar niet uit (de **blauwe** tabellen). In die gevallen kunnen voor een land verschillende antwoordmodaliteiten gelden. In de gevallen dat de antwoordmodaliteiten tegenhangers van elkaar zijn (bijvoorbeeld: een bepaalde omstandigheid is wel of niet van toepassing of aanwezig in het land) dan is slechts een van de antwoordmodaliteiten mogelijk. Ter verduidelijking zijn de modaliteiten, waarbij maar een van de twee kan gelden, in het **oranje** in de tabel opgenomen.

Gelet op het feit dat het onderzoek naar Spanje en Verenigd Koninkrijk geen informatie heeft opgeleverd over de onderwerpen waar het zwaartepunt van het onderzoek ligt (inzet dwangbevoegdheden, informatie verzamelen/delen, coördinatie en uitvoering dreigingsanalyse) en de gevonden informatie bovendien niet kon worden geverifieerd, zijn deze landen niet meegenomen in de landenvergelijking.

Daarnaast zijn voor de onderdelen ‘VIPS’ en ‘(kroon)getuigen’ niet opgenomen in de vergelijking. Beiden zijn in dit onderzoek kort behandeld, maar hiervoor wordt in de praktijk een eigen regime gehanteerd dat op vergelijkbare wijze wordt ingevuld in de verschillende landen. Voor het onderdeel VIPS is onvoldoende geverifieerde informatie beschikbaar om deze op te nemen in de landenvergelijking. Voor (kroon)getuigen geldt dat de focus van het onderzoek niet ligt op dit regime. Om een overzichtelijke en bruikbare vergelijking te maken, hebben wij ons daarom beperkt tot de andere onderdelen.

De vergelijking is uitgevoerd voor de volgende onderwerpen:

- De betrokken organisaties, hun onderlinge rolverdeling en -verhouding.
- De aanleiding voor de inzet van het stelsel.
- De dwangbevoegdheden om informatie te verzamelen.
- Het delen en verzamelen van informatie via andere organisaties of open bronnen.
- Het coördineren en uitvoeren van dreigingsanalyses.
- Het nemen, evalueren en afbouwen van maatregelen.
- Het uitoefenen van toezicht.

7.2 Onderwerpen en antwoordmodaliteiten

7.2.1 Betrokken organisaties, rolverdeling en -verhouding

In alle landen is de politie betrokken bij het stelsel van bewaken en beveiligen, bijvoorbeeld door het aanleveren van informatie voor dreigingsanalyses of het uitvoeren van de beveiliging.

Slechts één land heeft een speciale organisatie opgericht om het stelsel van bewaken en beveiligen te coördineren. Dit is de UCIS in Italië. De UCIS heeft verschillende taken, zoals het beoordelen van risicoanalyses, het evalueren van dreigingssituaties en het nemen van maatregelen. Italië maakt geen gebruik van een volledig centraal systeem, want zij wordt nog steeds op lokaal en regionaal niveau ondersteund door politie en prefecten, die verantwoordelijk zijn voor de openbare orde in een bepaald deelgebied van Italië. Het voordeel van een meer gecentraliseerde aanpak, is dat dit in de praktijk leidt tot betere informatiedeling en coördinatie van het stelsel. Dat is belangrijk voor een land als Italië dat veel te maken heeft met georganiseerde misdaad en veel personen moet voorzien van beveiligingsmaatregelen. Volgens de Italiaanse autoriteiten wordt relevante informatie door een meer gecentraliseerde aanpak op een effectievere wijze verzameld en kan het risico op een dreiging accurater worden ingeschat.

Denemarken is het enige land dat volledig centraal georganiseerd is. In Denemarken gaat de veiligheids- en inlichtingendienst hoofdzakelijk over het bewaken en beveiligen van personen. De dienst kan vergeleken worden met een combinatie van de Nederlandse organisaties AIVD, Dienst Koninklijke en Diplomatieke Beveiliging (DKDB) en NCTV. De Deense inlichtingendienst verzamelt de inlichtingen, stelt de analyses op, bepaalt welke maatregelen nodig zijn en voert de fysieke beveiliging vervolgens uit. Om die reden hoeft Denemarken weinig samenwerking tussen partijen te organiseren op dit onderwerp. Dit is opvallend, omdat alle andere landen in dit onderzoek in ieder geval met meerdere partijen samenwerken binnen het stelsel. Deze landen vertonen qua organisatie zowel centrale als decentrale kenmerken, waarbij bepaalde taken door een of meerdere centrale organisatie(s) worden uitgevoerd en/of gecoördineerd, en lokale autoriteiten, zoals de politie een rol spelen in bijvoorbeeld de uitvoering van de beveiliging. Ook kiezen landen als Italië, België en Frankrijk ervoor om de beslissing om het stelsel in te zetten te scheiden van de uitvoering van de bewakingsmaatregelen, net als het scheiden van taken wie een dreigingsanalyse uitvoert en wie bepaalt of het systeem mag worden ingezet.

In Duitsland wordt een onderscheid gemaakt tussen taken op federaal niveau en deelstaatniveau. Op federaal niveau is het Bundeskriminalambt verantwoordelijk voor de beveiliging van een gelimiteerde en specifieke groep personen. De overige taken zijn belegd bij de deelstaten. Alle deelstaten kennen eigen organisaties en wetten, maar federale wetgeving waaraan alle deelstaten gebonden zijn zorgt voor een zekere mate van uniformiteit tussen deelstaten. In de Duitse deelstaat Nedersaksen is de coördinatie en uitvoering van persoonsbescherming belegd bij een afdeling binnen het Landeskriminalambt die specifiek gericht is op bewaken en beveiligen van personen.

Opvallend aan Frankrijk is dat er een organisatie in het leven is geroepen om specifiek de samenwerking bij dreigingen vanuit terrorisme te coördineren (de UCLAT). Ook interessant is dat België ervoor heeft gekozen een organisatie op te richten die specifiek als taak heeft dreigingsanalyses voor veiligheidskwesties in het land (waaronder die voor bedreigde personen) te

coördineren. Ten slotte is België het enige land waarbij het nationale crisiscentrum een rol heeft in het stelsel, die vergelijkbaar is met de rol van de UCIS in Italië.[244]

Onderwerp	Modaliteit			
Betrokken organisaties (I)	*Politie* • Italië • België • Frankrijk • Denemarken • Duitsland	*Speciaal opgerichte organisatie*[245] • Italië	*Inlichtingendienst(en)* • Italië • België • Frankrijk • Denemarken	*Ministeries* • Italië • België • Frankrijk
Betrokken organisaties (II)	*Coördinerend orgaan antiterrorisme* • Frankrijk	*Nationaal Crisiscentrum* • België	*Coördinerend orgaan dreigingsanalyses* • België	*Dienst 25 LKA* • Duitsland
Rolverdeling & verhouding (I)	*Centraal georganiseerd* • Denemarken	*Zowel centrale als decentrale kenmerken* • Italië • België • Frankrijk • Duitsland		
Rolverdeling & verhouding (II)	*Uitvoering dreigingsanalyse en beslissing inzet stelsel organisatorisch gescheiden* • Italië • België • Frankrijk	*Uitvoering dreigingsanalyse en beslissing inzet stelsel bij dezelfde organisatie belegd* • Denemarken • Duitsland	*Beslissing inzet stelsel en uitvoering bewaking organisatorisch gescheiden* • Italië • België • Frankrijk	*Beslissing inzet stelsel en uitvoering bewaking belegd bij dezelfde organisatie* • Denemarken • Duitsland

[244] Het Nederlandse Nationaal CrisisCentrum (NCC) is een interdepartementaal coördinatiecentrum bij een (dreigende) crisis. Het NCC ondersteunt de crisisstructuur en is onderdeel van de NCTV.
[245] Met een speciaal opgerichte organisatie doelen wij op een organisatie die specifiek in het leven is geroepen voor het stelsel van bewaken en beveiligen.

7.2.2 Aanleiding inzet stelsel

Het proces rondom bewaken en beveiligen kan om verschillende redenen worden ingezet. Uit ons onderzoek is in ieder geval gebleken dat een aangifte in alle landen aanleiding kan zijn om het stelsel in te zetten. Voor België en Italië geldt dat signalen van andere betrokken organisaties het proces ook in gang kunnen zetten. In Italië kunnen er bijvoorbeeld signalen komen vanuit de lokale politie. In België worden signalen van de procureur gebruikt of kan informatie uit overleggen van het nationaal crisiscentrum een aanleiding zijn. Voor België, Italië en Denemarken is het van belang dat een betrokkene aangifte doet, omdat dit de juridische basis vormt voor het inzetten van strafrechtelijke dwangbevoegdheden en om informatie over het dreigingsbeeld te verzamelen. Het valt op dat in België ook signalen uit de media kunnen worden gebruikt.

Onderwerp	Modaliteit		
Aanleiding inzet stelsel	*Aangifte* • Italië • België • Frankrijk • Denemarken • Duitsland	*Signalen andere betrokken organisaties* • Italië • België	*Media* • België

7.2.3 Dwangbevoegdheden om informatie te verzamelen

Wat betreft de dwangbevoegdheden die organisaties hebben om informatie te verzamelen in het kader van de beveiliging van personen heeft Frankrijk daar een afzonderlijk regime voor. In Frankrijk vallen zowel de inlichtingendiensten als de politie onder de werking van de inlichtingenwet, die hen dwangbevoegdheden geeft om informatie te verzamelen als er sprake is van een terroristische dreiging, zoals het nemen van preventieve maatregelen en het instellen van beveiligingszones, voor surveillance en monitoring, het onderscheppen van communicatie en het inzetten van noodbevoegdheden. In België geldt voor de inlichtingendiensten dat specifiek in de wet is opgenomen dat zij dwangbevoegdheden kunnen inzetten voor de uitvoering van een beveiligingsopdracht van een persoon. Deze bevoegdheden mogen worden ingezet indien gewone methoden onvoldoende uitkomst bieden en de dwangbevoegdheid passend is gelet op de ernst van de dreiging.

In Italië en België wordt voor de politie volstaan met de ‘klassieke’ bevoegdheden die zij heeft in het kader van het strafrechtelijk onderzoek. Informatie kan daarmee niet op basis van een dwangbevoegdheid worden verzameld in het kader van de veiligheid van een persoon, maar kan alleen ingezet worden in lopende strafrechtelijke onderzoeken. Wanneer betrokkene aangifte doet kan de politie een strafrechtelijk onderzoek starten, waarna deze bevoegdheden kunnen worden ingezet. Gesloten strafrechtelijke onderzoeken waarbij dwangbevoegdheden in het verleden zijn ingezet kunnen wel dienen als bron van informatie. Voor Italië is niet gebleken dat de inlichtingendiensten specifiek dwangbevoegdheden kunnen inzetten, waaraan sec de veiligheid van personen ten grondslag

ligt. In het kader van terrorisme is het afluisteren van communicatie in Italië wel mogelijk met toestemming van de Procureur-generaal van het Hof van Beroep van Rome.

Hoewel de wetgeving in Denemarken specifiek een koppeling heeft gemaakt met het doen van onderzoek naar de beveiliging van personen door de inlichtingendienst, geldt dat voor de inzet van dwangbevoegdheden ook sprake moet zijn van een strafrechtelijk onderzoek. Grootste verschil met de andere landen is dat alleen de inlichtingendienst in het kader van de veiligheid van personen deze dwangbevoegdheden uitoefent en niet de politie.

In Nedersaksen beschikt Dienst 25 van het Landeskriminalamt over wettelijke bevoegdheden om informatie te vergaren voor het opstellen van risicoanalyses.

In geen van de onderzochte landen zijn andere organisaties aangetroffen die over dwangbevoegdheden beschikken, anders dan de politie[246] en inlichtingendiensten.

Onderwerp	Modaliteit			
Dwangbevoegdheden om informatie te verzamelen	*Er zijn dwangbevoegdheden specifiek voor het bewaken en beveiligen van personen* • Frankrijk • België (inlichtingendiensten)	*Er zijn geen specifieke dwangbevoegdheden voor het bewaken en beveiligen van personen* • Italië • België (politie) • Denemarken	*Politie heeft dwangbevoegd-heden* • Italië • België • Frankrijk • Spanje • Duitsland	*Inlichtingendienst heeft dwangbevoegdheden* • Italië • België • Frankrijk • Spanje • Denemarken

7.2.4 Informatie delen en verzamelen via andere organisaties en open bronnen

Voor het verzamelen van informatie op basis van open bronnen zijn in de onderzochte landen geen wettelijke bepalingen aangetroffen die dit expliciet reguleren. De grondslagen die hiervoor wordt gebruikt zijn algemenere bepalingen op basis waarvan de organisatie de bevoegdheid heeft om informatie te verzamelen. Voor het verzamelen en delen van informatie met/via andere organisaties bestaan in de onderzochte landen verschillende wettelijke bepalingen. Er is geen specifieke wet aangetroffen die enkel betrekking heeft op het delen en verzamelen van informatie in het kader van het bewaken en beveiligen van personen. De wettelijke basis om gegevens via andere organisaties te mogen verzamelen of te delen is aangetroffen in de wetgeving die taken van de politie en

[246] Hieronder valt ook de militaire politie (de equivalenten van de KMar), voor zover deze een rol vervult binnen de stelsels in de onderzochte landen. Dat is het geval in Italië en Frankrijk.

inlichtingendiensten reguleert en in wetgeving over andere betrokken organisaties die een taak vervullen binnen het stelsel, of daarvoor speciaal in het leven zijn geroepen zoals in Italië.

In Denemarken bevat de wet die de taken van de inlichtingendienst reguleert, grondslagen om open bronnen te raadplegen en informatie via andere organisaties te ontvangen. Hierin zijn ook regels opgenomen om informatie met andere overheden te delen. Ook in Frankrijk schept de inlichtingenwet grondslagen om informatie te verzamelen voor inlichtingendiensten, en te delen via administratieve overheden, lokale politiediensten en speciaal aangewezen functionarissen.

Voor Italië geldt dat de wetgeving rondom het instellen van de speciaal opgerichte organisatie (UCIS) grondslagen biedt hoe informatie via andere organisaties zoals inlichtingendiensten vergaard kan worden. In België is er een vergelijkbare wet waarin is geregeld dat politie en inlichtingendiensten gegevens mogen delen met de organisatie die de coördinatie voert op de dreigingsanalyses (OCAD). Daarnaast bevat de wet regels voor inlichtingendiensten en de wet op het Politieambt, grondslagen voor de inlichtingendiensten en de politie om gegevens te mogen delen.

In Duitsland zijn bevoegdheden om informatie te vergaren neergelegd in het federale Strafprozeßordnung (Wetboek van Strafvordering) en de Politiewetten van de deelstaten.

Qua vorm waarin de informatie wordt gedeeld, geldt voor Frankrijk en Denemarken dat dit op schriftelijke wijze gebeurt. Voor België geldt dat informatie met OCAD voornamelijk schriftelijk wordt gedeeld. Vervolgens ontvangt de NCCN alleen de dreigingsanalyse en mondeling informatie via overleg. In Italië gebeurt het uitwisselen van de informatie met name mondeling. Daarnaast worden relevante antwoorden op vragen van de UCIS schriftelijk gedeeld, zonder daarbij de onderlinge vertrouwelijke stukken prijs te hoeven geven.

Onderwerp	Modaliteit		
Informatie verzamelen	*Via open bronnen* • Italië • Frankrijk • Denemarken • België • Duitsland		
Informatie verzamelen en delen	*Via/met andere organisaties* • Italië • België • Frankrijk • Denemarken • Duitsland	*Wettelijk vastgelegd* • Frankrijk • Denemarken • Italië • België • Duitsland	

Informatie delen (vorm)	*Vertrouwelijke informatie wordt mondeling gedeeld* • Italië • België	*Vertrouwelijke informatie wordt schriftelijk gedeeld* • België • Frankrijk • Denemarken	*Slechts de relevante antwoorden worden gedeeld (hit/no hit)* • Italië

7.2.5 Dreigingsanalyses

Voor de dreigingsanalyses geldt dat in alle landen waar deze informatie beschikbaar is, wordt gewerkt met verschillende dreigingsniveaus.

Wat betreft terroristische dreigingen is het opvallend dat zowel Italië, België als Frankrijk werken met een specifieke organisatie die het uitvoeren van de dreigingsanalyse coördineert. Bij deze organisatie komt de informatie die is verzameld door verschillende betrokken partijen samen. De precieze rol van die organisatie, en op welke wijze deze informatie met haar wordt gedeeld (zie hiervoor) verschilt wel per land. Zo voeren in België (OCAD) en Frankrijk (UCLAT) de dreigingsanalyses deels zelf uit op basis van de vertrouwelijke informatie die ze verkrijgen van de politie en inlichtingendiensten, terwijl in Italië deze organisatie (UCIS) slechts de door de politie gemaakte dreigingsanalyse beoordeelt ten behoeve van de uitvoering van de beschermingsmaatregelen. In België maakt de NCCN vervolgens op vergelijkbare wijze een beoordeling van de dreigingsanalyse die (deels) door de OCAD is uitgevoerd en gecoördineerd. Door de scheiding tussen uitvoering en beoordeling van de dreigingsanalyse is het in Italië niet nodig om de onderliggende vertrouwelijke informatie waarop de dreigingsanalyse is gebaseerd schriftelijk te delen. Nadere vragen of verzoeken tot informatie vanuit de UCIS kunnen door de politie mondeling of schriftelijk worden beantwoord. In België geldt hetzelfde voor het delen van informatie met de NCCN. Voor Nedersaksen geldt dat er geen speciale organisatie is opgericht voor coördinatie en uitvoering, maar deze taak is wel belegd bij een specifieke afdeling binnen het Landeskriminalambt en stelt dreigingsanalyses op en neemt maatregelen op basis van politie-informatie.

In Denemarken ziet coördinatie er anders uit, doordat het systeem gecentraliseerd is. Gezien zowel het vergaren van de informatie als het maken van de dreigingsanalyse en de beoordeling daarvan ten behoeve van de uitvoering van beschermingsmaatregelen bij de inlichtingendienst is belegd, is het minder nodig voor deze organisatie om samenwerking en het delen van informatie met andere betrokken partijen te organiseren.

Qua uitvoering van de dreigingsanalyse springt Italië eruit, omdat de politie bij terrorisme ook het voortouw heeft om de dreigingsanalyse voor een bepaalde bedreigde persoon op te stellen, terwijl in België, Frankrijk en Denemarken de inlichtingendiensten en/of de coördinerende organisaties hierover gaan. In Italië levert de inlichtingendienst op dit gebied met name informatie op het niveau van fenomenen, bijvoorbeeld over de aard van een bepaalde terroristische groepering.

In het geval van georganiseerde misdaad geldt in België en Italië dat er coördinatie wordt gevoerd door dezelfde organisatie als bij terroristische dreigingen. De uitvoering van de dreigingsanalyse wordt in België door een afdeling van de politie en OCAD gezamenlijk gedaan. In Italië is alleen de politie belast

met de uitvoering van de dreigingsanalyse. In Frankrijk ontbreekt deze coördinatie op het gebied van georganiseerde misdaad, en wordt de dreigingsanalyse door de politie uitgevoerd. Denemarken wijkt in het kader van georganiseerde misdaad het meeste af qua werkwijze, omdat de inlichtingendienst wat betreft georganiseerd misdaad ook de dreigingsanalyse uitvoert, en niet de politie.

Onderwerp	Modaliteit				
Dreigingsanalyse (coördinatie)	*Een organisatie voert de coördinatie bij de uitvoering van de dreigingsanalyse bij terrorisme uit* • België • Italië • Frankrijk • Denemarken • Duitsland	*Een organisatie voert de coördinatie bij de uitvoering van de dreigingsanalyse bij georganiseerde misdaad uit* • België • Italië • Denemarken • Duitsland	*Er vindt geen coördinatie plaats bij georganiseerde misdaad* • Frankrijk		
Dreigingsanalyse bij terrorisme (uitvoering)	*Dreigingsanalyse werkt met verschillende niveaus* • Italië • België • Frankrijk • Denemarken • Duitsland	*Dreigingsanalyse over te beveiligen persoon wordt door meerdere organisaties gemaakt* • België • Frankrijk	*Dreigingsanalyse over te beveiligen persoon wordt door één organisatie gemaakt* • Italië • Denemarken	*Politie maakt dreigingsanalyse over te beveiligen persoon* • Italië	*Inlichtingendienst maakt dreigingsanalyse over te beveiligen personen* • België • Frankrijk • Denemarken
Dreigingsanalyse bij georganiseerde misdaad (uitvoering)	*Dreigingsanalyse werkt met verschillende niveaus* • Italië • België • Frankrijk • Duitsland	*Dreigingsanalyse over te beveiligen persoon wordt door meerdere organisaties gemaakt* • België • Frankrijk	*Dreigingsanalyse over te beveiligen persoon wordt door één organisatie gemaakt* • Italië • Denemarken	*Politie maakt dreigingsanalyse over te beveiligen persoon* • Italië • België • Frankrijk	*Inlichtingendienst maakt dreigingsanalyse over te beveiligen persoon* • Denemarken

7.2.6 Maatregelen nemen, evalueren en afbouwen

Uit de verkenning blijkt dat het per land verschilt welke organisatie of persoon bevoegd is om te beslissen of beveiligingsmaatregelen voor bedreigde personen worden ingezet. Dit is een andere vraag dan wie beslist wat de inhoud van deze maatregelen is. Ook verschilt het of deze bevoegdheid is belegd bij één organisatie of meerdere. Voor alle onderzochte landen geldt dat de dreigingsanalyse de basis is voor de te nemen maatregelen. Hoe deze precies doorwerkt in de uiteindelijk te nemen maatregelen verschilt wel per land.

Voor Italië geldt dat zowel de speciaal opgerichte organisatie (de UCIS) als de prefect oordelen of maatregelen ingezet moeten worden. Hoewel er standaardpakketten zijn, verschilt het per dreigingsniveau of maatregelen vooraf vaststaan of dat een afweging nodig is gebaseerd op de specifieke omstandigheden van een situatie. Opvallend aan Italië is dat zij dus niet strikt gehouden zijn aan de dreigingsniveaus en maatregelen, maar er ook ruimte is voor maatwerk. Het is in Italië dan ook mogelijk dat aanvullende of andere maatregelen die niet passen in het dreigingsniveau gerechtvaardigd zijn. Om maatregelen te kunnen ontvangen tekent de te beveiligen persoon een standaardcontract. Hierin staan de plichten staan waar hij zich aan moet houden. Er is geen ruimte voor maatwerk. Gaat iemand niet akkoord, dan ontvangt hij ook geen beveiliging. Die plichten zien niet alleen op het opgeven van vrijheden, maar ook op het akkoord gaan met de typen maatregelen. De te beveiligen persoon kan niet een deel van zijn maatregelenpakket (bijvoorbeeld de escortes) weigeren. Voor andere landen is deze informatie niet beschikbaar, dus een vergelijking maken is niet mogelijk.

In Frankrijk beslist de minister van Binnenlandse Zaken of maatregelen worden ingezet. Het is niet bekend of Frankrijk gebruikmaakt van standaardpakketten of maatwerk per te beveiligen persoon. De minister oordeelt op basis van dreigingsanalyses en ontvangt advies van een commissie bij het bepalen van de inhoud van de maatregelen. In deze commissie nemen de directeur-generaal van de Nationale Politie, de directeur-generaal van de Nationale Gendarmerie, de prefect van de Parijse politie, het hoofd van de beschermingsdienst en de directeur-generaal van de Interne Veiligheid. Het is mogelijk dat de minister van Binnenlandse Zaken ook zonder advies van de commissie beslist om beveiligingsmaatregelen te treffen.

In België is het Nationaal Crisiscentrum bevoegd om te oordelen of maatregelen worden ingezet. Het NCCN maakt een dreigingsevaluatie op basis van informatie die zij van het OCAD en een afdeling van de politie ontvangt. Op basis van het dreigingsniveau, dat kan variëren van 1 tot 4, wordt bepaald welke maatregelen in een bepaalde situatie passend zijn. Dat kan variëren van een lichte vorm (een contactpersoon aanstellen bij de lokale positie) tot uitzonderlijke gevallen (24/7 persoonsbescherming). Voor niveau 4 geldt dat de Federale politie bepaalt of een beschermingscommissie wordt ingesteld om te adviseren over extreme gevallen. Hier wordt een dreigingsniveau niet gekoppeld aan een bepaalde set maatregelen, maar ondersteunt de hoogte van het dreigingsniveau de inzet van bepaalde maatregelen. Zo rechtvaardigt het zwaarste dreigingsniveau (4) uitzonderlijke maatregelen, zoals tijdelijke of permanente identiteitswijziging. Voor België geldt ook dat dit crisiscentrum het initiatief neemt om casusoverleggen met verschillende diensten in te plannen. Het is echter opvallend dat voor de diensten geen formele plicht betstaat om aan de overleggen deel te nemen. Uit de ervaring van het NCCN is gebleken dat diensten zonder deze

verplichting wel meewerken. Opvallend is dat er tijdens dit overleg ook ruimte is om bijvoorbeeld de mentale gezondheid van de bedreigde persoon te bespreken en er oog is voor de impact op de familie.

Aangezien Denemarken een gecentraliseerd stelsel van bewaken en beveiligen hanteert, ligt het voor de hand dat de keuze om maatregelen in te zetten ligt bij de PET. Deze organisatie is immers verantwoordelijk voor het bewaken en beveiligen van personen en draagt de meeste taken op dit gebied uit. Daarmee beslist PET ook welke maatregelen worden ingezet.

Onderwerp	Modaliteit			
Maatregelen (beslissen)	*Prefect beslist of aanvullende maatregelen worden genomen* • Italië	*Speciaal opgerichte organisatie beslist of maatregelen worden genomen* • Italië	*Minister / Ministerie beslist of maatregelen worden genomen* • Frankrijk	*Nationaal Crisiscentrum beslist of maatregelen worden genomen* • België
Maatregelen (inhoud)	*Er worden beveiligingsmaatregelen getroffen op basis van dreigingsanalyse* • België • Denemarken • Frankrijk • Italië	*Er zijn standaardpakketten maatregelen afhankelijk van het dreigingsniveau* • Italië	*Naast standaard-maatregelen kunnen aanvullende / afwijkende maatregelen worden getroffen* • Italië	*Per casus wordt een afweging gemaakt welke maatregelen nodig zijn* • België • Denemarken
Plichten te bewaken persoon	*Niet bekend* • Frankrijk • België • Denemarken	*Standaardcontract* • Italië	*Geen contract*	*Maatwerkcontract*

In alle onderzochte landen vindt evaluatie van de maatregelen en de dreigingsanalyse plaats. Dat gebeurt in ieder geval als er nieuwe informatie beschikbaar is. Hetzelfde geldt voor het afbouwen van maatregelen.

In België en Italië worden lopende casussen elke drie maanden besproken, tenzij een gebeurtenis (zoals een arrestatie) plaatsvindt die eerder overleg noodzakelijk maakt. In Italië is het ook mogelijk dat een casus een keer per zes maanden wordt besproken. Uit het onderzoek is niet gebleken dat maatregelen in een keer volledig stop kunnen worden gezet. Daarvoor vinden overleggen plaats waarin het afbouwen van maatregelen wordt besproken. Een wijziging in de dreigingssituatie betekent dus niet dat een te beschermen persoon van het een op het andere moment zijn beveiliging kan verliezen. Voor Italië geldt dat wanneer wordt getwijfeld of de maatregelen afgebouwd moeten worden in een bepaalde casus, een adviescomité ingeschakeld kan worden.

Onderwerp	Modaliteit				
Evaluatie van maatregelen en bijstellen dreigingsanalyse	*Er vindt evaluatie van de maatregelen / dreigingsanalyses plaats* • België • Denemarken • Frankrijk • Italië • Duitsland	*Er vinden vaste periodieke overleggen plaats om maatregelen te evalueren* • België • Italië	*Er vinden overleggen plaats naar aanleiding van nieuwe informatie/ incidenten* • België • Italië		
Afbouwen van maatregelen	*Maatregelen worden afgebouwd op basis van nieuwe informatie* • Italië • België • Frankrijk • Denemarken	*Voor de afbouw van maatregelen wordt advies ingewonnen* • Italië	*Maatregelen worden geleidelijk afgeschaald* • Italië	*Er vinden overleggen plaats om maatregelen af te bouwen* • Italië • België	

7.2.7 Toezicht

Toezicht op het stelsel van bewaken en beveiligen wordt in de onderzochte landen op verschillende manieren geregeld.

Frankrijk heeft een adviesorgaan ingesteld als onafhankelijk toezichthouder. Dit onafhankelijk orgaan kan zowel vooraf, niet-bindend advies uitbrengen over de bevoegdheden van inlichtingendiensten, als achteraf toezicht uitoefenen. Voor toezicht achteraf heeft zij permanente, volledig en directe toegang tot relevante gegevens. Bij onregelmatigheden informeert dit orgaan de premier. Ook het Verenigd Koninkrijk maakt gebruik van een officiële toezichthouder om misbruik van surveillance- en inlichtingenbevoegdheden in kaart te brengen. Een belangrijk verschil tussen deze landen is dat de Britse toezichthouder geen adviesorgaan is (zoals in Frankrijk), maar een onafhankelijk gerechtelijk orgaan dat klachten behandelt. Een schending moet dus eerst tot een klacht hebben geleid voordat de Britse toezichthouder zich hierover kan buigen. In Frankrijk kan dit orgaan dus wel vooraf advies geven, ook al is dit niet bindend.

Denemarken kent een soortgelijke parlementaire commissie die het doel heeft om toezicht te houden op de Deense inlichtingendiensten. De commissie adviseert de regering mondeling of schriftelijk over de behandelde aangelegenheden. Haar bevoegdheden zijn dankzij een recente wetswijziging versterkt. In België is het toezicht ook (deels) geregeld via parlementaire commissies. België kent twee verschillende comités die toezicht houden op de politie- en inlichtingendiensten.

In België zijn twee vaste comités verantwoordelijk voor het toezicht op de deelnemende partijen van het stelsel van bewaken en beveiligen, ook wat betreft de bescherming van persoonsgegevens. In Duitsland is externe controle geregeld via parlementair toezicht.

De enige instantie die geen officiële toezichthouder heeft in de vorm van commissies of autoriteiten, is Italië. Daar vindt toezicht plaats in de vorm van ministeriële verantwoordelijkheid. De minister van Binnenlandse Zaken is eindverantwoordelijk.

Het schema wordt weergegeven op de volgende pagina.

Onderwerp	Modaliteit			
Toezicht	*Geen onafhankelijk toezichthouder* • Italië	*Er is een onafhankelijk toezichthouder* • Denemarken • Frankrijk	*Toezicht via ministeriële verantwoordelijkheid* • Italië	*Toezicht via parlementaire commissie* • België • Denemarken • Duitsland

8. Conclusie

In dit hoofdstuk wordt antwoord gegeven op deelvragen 5 en 6. Bij de beantwoording van deze vragen is geput uit de analyse per land en de landenvergelijking. Allereerst gaan we op basis van de bevindingen in op wat er op hoofdlijnen van de verschillende landen te leren valt wat betreft de stelsels van bewaken en beveiligen (deelvraag 5). Daarbij wordt de juridische analyse van de artikelen 2 en 8 van het EVRM betrokken. Daarna beschrijven we de inspiratie voor het wetsvoorstel die kan worden opgedaan uit de onderzochte landen (deelvraag 6). Dit doen we aan de hand van een referentiemodel, dat bestaat uit de ijkpunten die voortvloeien uit de bevindingen. Deze ijkpunten worden vervolgens ingekleurd met voorbeelden die we uit deze landenverkenning hebben opgehaald.

8.1 Bevindingen

De onderzochte landen kennen allemaal een stelsel van bewaken en beveiligen van bedreigde personen door andere personen of groeperingen. De oorzaken van de dreigingen zijn divers en elk land kent hierbij zijn eigen maatschappelijke en historische context die van invloed is geweest op de ontwikkeling en vormgeving van het stelsel. In het onderzoek hebben we de focus gelegd op dreigingen die voortkomen uit terroristische of criminele motieven.

Op Denemarken na – waar gekozen is voor een gecentraliseerde aanpak – zijn er in de onderzochte landen meerdere organisaties betrokken die vanuit ieders taak een rol vervullen binnen het stelsel van bewaken en beveiligen. Het kunnen delen van informatie tussen deze organisaties is noodzakelijk om de dreiging te analyseren, het dreigingsniveau te kunnen vaststellen, en de beschermingsmaatregelen te kunnen treffen, evalueren en uiteindelijk te kunnen afbouwen. Uit gesprekken is gebleken dat het daarbij van essentieel belang is dat een van de organisaties de samenwerking in de keten en het samenkomen van informatie coördineert, zodat een organisatie verantwoordelijk is voor het samenbrengen van alle losse puzzelstukjes.

De onderzochte landen hebben specifieke wetgeving die een grondslag bieden om zowel structureel als incidenteel informatie, waaronder persoonsgegevens, te verzamelen en te kunnen delen. Het gaat daarbij om informatie afkomstig uit lopende onderzoekdossiers en dus niet om het verzamelen en delen van informatie over de bedreiging tegen een bepaald persoon. Dit is slechts anders wanneer een betrokkene aangifte heeft gedaan van bijvoorbeeld bedreiging of geweld en er naar aanleiding van die aangifte reeds een strafrechtelijk onderzoek is gestart. Vanaf dat moment kunnen dwangbevoegdheden worden aangewend door de politie. Enige uitzondering hierop is Frankrijk, waar in het geval van een terroristische dreiging de politie bepaalde dwangbevoegdheden heeft. Overigens hebben de onderzoekers in geen van de landen een uitbreiding van de dwangbevoegdheden van de ondersteunende diensten aangetroffen specifiek gericht op de situatie dat een persoon wordt bedreigd.

Wat opvalt is dat met uitzondering van Denemarken de organisaties die het dreigingsniveau en de te treffen beschermingsmaatregelen vaststellen niet beschikken over dwangbevoegdheden om informatie te verzamelen en evenmin toegang lijken te hebben tot vertrouwelijke informatie, maar enkel beschikken over de uitkomst van de gemaakte analyse van de dreiging. Op deze wijze wordt

bedoeld of onbedoeld invulling gegeven aan het beginsel van dataminimalisatie uit de AVG en de richtlijn gegevensbescherming bij rechtshandhaving.

In twee van de onderzochte landen hebben we kunnen vaststellen dat er een casusoverleg wordt gehouden. Dergelijke overleggen zijn volgens de gesprekspartners zeer behulpzaam om tot effectieve samenwerking te komen en om elkaar snel op vlieghoogte te brengen. Het karakter daarvan kan technisch dan wel evaluerend van aard zijn. Een dergelijk casusoverleg geeft – afhankelijk van de inrichting en de deelnemers van het overleg – ook ruimte om aandacht te besteden aan bijvoorbeeld de mentale gezondheid van de bedreigde persoon en de impact op zijn familieleden.

In de onderzochte landen vindt in verschillende vormen toezicht plaats. In een aantal landen zijn onafhankelijke toezichthoudende autoriteiten aangewezen die toezicht houden op de verwerking van persoonsgegevens bij het inzetten van instrumenten door veiligheidsdiensten dan wel de gegevensverwerking door het coördinatieorgaan voor de dreigingsanalyse. In andere landen vindt het toezicht plaats door het parlement of door comités, waarin vanuit verschillende disciplines zitting wordt genomen, dan wel door de verantwoordelijk minister. Naast de laatstgenoemde vormen van toezicht vindt ook onafhankelijk toezicht plaats op de verwerking van persoonsgegevens door toezichthoudende autoriteiten aangewezen op grond van de uitvoerings- en implementatiewetgeving van de AVG en de richtlijn.

De onderzochte landen hebben het stelsel van bewaken en beveiligen op zodanige wijze georganiseerd dat de randvoorwaarden aanwezig zijn om binnen de kaders die het EHRM stelt invulling te geven aan de uit artikel 2 van het EVRM voortkomende positieve verplichting van de staat om het leven van personen te beschermen die onder zijn jurisdictie vallen. Zo is er in de regelgeving van de landen en in de praktijk voorzien in het kunnen delen van gegevens tussen de betrokken instanties, waardoor het mogelijk zou moeten zijn om over concrete kennis te beschikken om reële en onmiddellijke risico's te onderkennen en operationele maatregelen te treffen. Uit het onderzoek is niet naar voren gekomen dat op grond daarvan ook preventieve maatregelen worden getroffen. Vanwege de reikwijdte van het onderzoek hebben de onderzoekers geen inzicht verkregen in hoe het stelsel in het licht van de jurisprudentie van het EHRM – in het bijzonder het Osman-criterium – in individuele casusposities uitpakt.

Het verwerken van persoonsgegevens in het kader van het beschermen van bedreigde personen, vormt een inmenging op de persoonlijke levenssfeer van de betrokkene. Het gaat daarbij niet alleen om de bedreigde persoon zelf, maar ook om de persoon of groepering die de bedreiging vormt. In een belangrijk deel van de onderzochte landen is de grondslag van de inmenging op de persoonlijke levenssfeer opgenomen in een wet in formele zin met een verdere uitwerking in lagere regelgeving of in beleid en richtlijnen, waarin in gepreciseerd is onder welke omstandigheden en voorwaarden door de verschillende overheidsorganisaties een inbreuk kan worden gemaakt in verband met het beschermen van de bedreigden persoon. Geen van de landen heeft specifieke wetgeving gericht op het stelsel van bewaken en beveiligen en gegevensdeling binnen dat stelsel. De regelgeving daaromtrent is ondergebracht in verschillende materiewetten, waarin de taken en bevoegdheden van de verschillende organisaties zijn vastgelegd. In dat licht moet wel worden opgemerkt dat voor onderzoek in online publiek toegankelijke bronnen in de onderzochte landen met gebrek aan specifiek daarop gerichte bepalingen wordt teruggevallen op meer generieke bevoegdheden ten aanzien waarvan een vertaalslag moet worden gemaakt naar de toepassing in de digitale wereld. Of de

informatievergaring in het individuele geval voldoet aan de eisen van proportionaliteit en subsidiariteit hebben de onderzoekers niet kunnen vaststellen, omdat het onderzoek zich richt om inzicht te krijgen in de werking van het stelsel van bewaken en beveiligen in de onderzochte landen.

8.2 Inspiratie voor het (concept)wetsvoorstel eigenstandige bevoegdheden

In dit hoofdstuk hebben wij een referentiemodel gecreëerd met ijkpunten die voortkomen uit de bevindingen van het onderzoek. Het referentiemodel kan gebruikt worden ter inspiratie voor een (concept)voorstel van eigenstandige bevoegdheden in Nederland om op een verantwoorde manier informatie te delen in het stelsel van bewaken en beveiligen. Het is daarbij van belang dat informatiedeling wordt gezien in een bredere context en niet alleen als een juridische, op zichzelf staande bevoegdheid. Aan de hand van het referentiemodel laten wij zien dat de verschillende onderzochte onderdelen van het stelsel van belang zijn om verantwoorde en efficiënte gegevensdeling mogelijk te maken. In een dergelijk systeem met 'checks-and-balances' wordt op verschillende momenten in het proces gegevensdeling op verantwoorde wijze mogelijk gemaakt dan wel gecontroleerd, van het moment dat het stelsel wordt ingezet, tot aan het toezicht daarop achteraf.

Per ijkpunt leggen we uit welke dilemma's daarbij spelen qua inrichtingskeuzes en lichten we een of meerdere landen uit ter inspiratie voor het stelsel in Nederland. De ijkpunten zijn geformuleerd aan de hand van de onderwerpen die in hoofdstukken 6. en 7. centraal stonden.

Daarnaast moet worden opgemerkt dat het stelsel van een bepaald land in diens eigen context bekeken moet worden, bijvoorbeeld in relatie tot de cultuur en hoe organisaties en het betreffende stelsel zijn ingericht. Het overnemen van een best practice uit land A hoeft daarom geen automatisch succes te betekenen voor land B. In dit referentiemodel nemen we elementen die kunnen bijdragen aan een goede werking van het stelsel, maar het is nodig om vanuit de Nederlandse context te bekijken of en hoe deze elementen optimaal kunnen werken.

Hierbij dient opgemerkt te worden dat we verschillende hoeveelheden aan informatie per land hebben kunnen verzamelen. Het kan dus zijn dat we voor een bepaald element niet (precies) weten hoe het in een land geregeld is, en dat we daarom een ander land als voorbeeld kiezen. Dat betekent niet dat het in een ander land minder goed is geregeld.

Daarnaast moet worden opgemerkt dat het stelsel van een bepaald land in diens eigen context bekeken moet worden, bijvoorbeeld in relatie tot de cultuur en hoe organisaties en het betreffende stelsel zijn ingericht. Het overnemen van een best practice uit land A hoeft daarom geen automatisch succes te betekenen voor land B. In dit referentiemodel nemen we elementen die kunnen bijdragen aan een goede werking van het stelsel, maar het is nodig om vanuit de Nederlandse context te bekijken of en hoe deze elementen optimaal kunnen werken.

Op de volgende pagina hebben we het referentiemodel eerst op schematische wijze uitgewerkt. Onder het schema volgt per ijkpunt de nadere uitwerking.

Referentiemodel voor het stelsel bewaken en beveiligen

IJkpunten	Elementen van landen ter inspiratie	Dilemma
1. Toegang tot het stelsel is adequaat	• België	Enerzijds moet het stelsel voor iedereen die te maken heeft met een dreiging gemakkelijk toegankelijk zijn, anderzijds is het niet wenselijk om veel middelen in te zetten bij dreigingen die niet reëel zijn.
2. Coördinatie tussen partijen is adequaat en rolverdeling is helder	• Italië • België • Duitsland	Enerzijds is het voor coördinatie wenselijk om zoveel mogelijk organisaties op één plek bij elkaar hebben of niet te veel deelnemers te hebben (makkelijker, efficiënter), anderzijds brengt deelname van meerdere organisaties, verschillende expertise mee die van belang of van toegevoegde waarde kunnen zijn.
3. Er is een heldere juridische basis voor het verzamelen en delen van informatie	• Denemarken • Duitsland	Aan de ene kant is er een groot belang om zoveel mogelijk relevante informatie te verzamelen en te delen en aan de andere kant speelt het belang van de persoonlijke levenssfeer, en gegevensbescherming die juist vragen om dataminimalisatie.
4. Er is een heldere juridische basis voor de inzet van dwangbevoegdheden	• Denemarken • Frankrijk • Duitsland	Aan de ene kant is er behoefte om informatie te kunnen verzamelen door middel van verschillende dwangbevoegdheden, aan de andere kant grijpen deze bevoegdheden zeer in op de persoonlijke levenssfeer en dienen deze middelen alleen ingezet te worden wanneer dat noodzakelijk en proportioneel is.
5. De dreigingsanalyse is adequaat/ bruikbaar	• Italië	Aan ene kant kan de dreiging het beste in beeld worden gebracht als zoveel mogelijk verschillende

	• België	typen informatie snel onderling wordt gedeeld, aan de andere kant is het om verschillende redenen onwenselijk als de overheid op grondslag van het maken van een dreigingsanalyse voor het bewaken en beveiligen van personen, in een bredere context informatie verzamelt en daar ook (via andere organisaties) gevolg aan laat geven.[247]
6. De evaluatie van maatregelen is effectief	• Italië • België	Het is enerzijds belangrijk om periodiek maatregelen te herzien of de mogelijkheid te hebben om snel in te grijpen wanneer de omstandigheden veranderen, maar anderzijds wil je ook niet vaker met elkaar om de tafel dan noodzakelijk is (over-evaluatie).
7. Het toezicht is eenduidig en doeltreffend	• Frankrijk	Balans tussen gesloten (vanwege gevoelige aard van werkzaamheden B&B) en een open karakter (voor het kunnen afleggen van verantwoording en transparantie).

1. Toegang tot het stelsel is adequaat

Bedreigde personen moeten op adequate wijze toegang kunnen krijgen tot het stelsel zodat bij de signalering van een bepaalde dreiging snel over kan worden gegaan tot het uitvoeren van een dreigingsanalyse en de eventuele inzet van beveiligingsmaatregelen. Een dilemma dat speelt bij het organiseren van de inzet van het stelsel is dat er een balans moet worden gevonden. Deze balans ligt in de toegankelijkheid van het stelsel. Voorkomen moet worden dat de beschikbare middelen niet adequaat worden ingezet omdat de drempel van toegang zo laag is dat er tijd verloren gaat aan het onderzoeken van niet reële dreigingen. Anderzijds moet het stelsel wel toegankelijk blijven voor daadwerkelijk bedreigde personen. In veel landen is het (onder meer) om die reden nodig om als bedreigde persoon een aangifte te doen.

Wat betreft de toegang tot het stelsel lichten wij België eruit. Nadat een persoon in België aangifte heeft gedaan wordt deze doorgezet naar het NCCN, waarna het NCCN de dreiging verder oppakt en zorgt dat het proces in gang wordt gezet, door een dreigingsanalyse te vragen van OCAD en/of DJO.

[247] Bijvoorbeeld dat tijdens het tappen van telefonisch verkeer wordt gesproken over een ander.

Signalen van een dreiging komen niet alleen bij het NCCN door middel van een aangifte. Daarnaast kan het NCCN van een dreiging op de hoogte raken door bijvoorbeeld signalen uit de pers, van de procureur of uit het overleg tussen het NCCN en de kabinetten van ministers.

2. Coördinatie tussen partijen is adequaat en rolverdeling is helder

Adequate coördinatie en een duidelijke rolverdeling zijn noodzakelijk voor de betrokken partijen in het stelsel van bewaken en beveiligen om tijdig en op een goede manier hun taken uit te kunnen voeren. Het is hierbij van belang dat duidelijk is welke rol een organisatie op zich neemt, zodat andere partijen weten wanneer zij betrokken moeten worden, informatie moeten aanleveren of beslissingen moeten nemen. Doorgaans zijn bij het stelsel van bewaken en beveiligen verschillende partijen betrokken. Het kan daarom raadzaam zijn om één organisatie als coördinerend orgaan aan te wijzen waar verschillende bronnen van informatie samenkomen. Enerzijds is het voor een centrale coördinatie wenselijk om zoveel mogelijk expertises op één plek bij elkaar hebben of niet te veel externe deelnemers te hebben (om makkelijker en efficiënter te overleggen), anderzijds brengt – in stelsels waar deze expertises niet binnen één organisatie zijn belegd - de deelname van meerdere organisaties, specialistische kennis met zich mee die van belang of van toegevoegde waarde kan zijn.

Ter toelichting lichten we Italië, België en Duitsland (deelstaat Nedersaksen) eruit. Voor Italië en België geldt dat beide landen gebruik maken van een orgaan dat aangewezen is om het stelsel te coördineren, maar dat hiervoor wel de input van verschillende gespecialiseerde organisaties gebruikt en regelmatig overlegt met betrokken stakeholders. Duitsland maakt gebruik van een aparte afdeling binnen de politie (het Landeskriminalamt).

In Italië is een speciaal coördinerend orgaan opgericht in het kader van bewaken en beveiligen (UCIS). Dit orgaan voert zelf geen onderzoek uit, maar ontvangt informatie van andere partijen. Deze informatie komt vanuit verschillende silo's bij het orgaan op één centraal punt terecht, waardoor het orgaan over alle benodigde informatie beschikt om de juiste maatregelen te treffen. In technische (vaak mondelinge) overleggen schuiven altijd de lokale politiediensten en de prefect aan.

In België komt de belangrijkste informatie op één plek terecht, namelijk bij het NCCN. OCAD en DJO leveren hiervoor vanuit hun eigen expertise de belangrijkste informatie aan. Ook aanvullende informatie kan via een verzoek bij OCAD of DJO worden opgehaald. Op initiatief van het NCCN vinden casusoverleggen plaats met alle diensten. Door één orgaan aan te wijzen voor coördinatie maar tegelijkertijd wel de informatie van verschillende diensten te benutten, wordt overzicht bewaard en kunnen dreigingen adequaat worden ingeschat.

In Nedersaksen is de taak van het bewaken en beveiligen belegd binnen een aparte afdeling (Dienst 25) van het Landeskriminalmt. Deze afdeling is specifiek en uitsluitend belast met bewaken en beveiligen in Nedersaksen. Hier worden de dreigingsanalyses gemaakt en wordt er besloten tot maatregelen op basis van reeds bestaande politie-informatie. Deze keuze vereenvoudigt de coördinatie van de activiteiten. De taken rondom bewaken en beveiligen zijn immers niet verdeeld over verschillende partijen waardoor coördinatie vooral binnen Dienst 25 plaatsvindt. De wet geeft daarnaast ook bevoegdheden aan Dienst 25 om zelf informatie te vergaren om risicoanalyses te kunnen opstellen. Omdat Dienst 25 onderdeel uitmaakt van de Nedersaksische politieorganisatie kan politie informatie zonder belemmering worden gedeeld.

3. Er is een heldere juridische basis voor het verzamelen en delen van informatie

Voor een goede informatieverzameling- en deling is het nodig dat de verschillende betrokken partijen weten welke informatie (uit open bronnen en van andere organisaties) zij mogen verzamelen en met welke partijen zij deze informatie onderling mogen delen en waar de grens ligt. Wat daarbij helpt is een heldere juridische basis waarin is bepaald voor welk (gezamenlijk) doel, welke gegevens met welke partijen voor welke taak kunnen worden gedeeld en welke waarborgen daarbij in acht worden genomen.

Een dilemma dat hierbij speelt is het vinden van de juiste balans tussen enerzijds het belang dat is gemoeid met het verzamelen en onderling delen van zoveel mogelijk relevante informatie, en anderzijds het belang om de inbreuk op persoonlijke levenssfeer van de verschillende betrokkenen te beperken tot wat noodzakelijk is, en vanuit het oogpunt van gegevensbescherming dataminimalisatie in acht te nemen.

Een goed voorbeeld van een land dat dit tot uitdrukking heeft gebracht is Denemarken, in de PET-wet. In deze wet is bepaald dat informatie uit open bronnen (hoewel impliciet) en van andere organisaties mag worden verzameld voor de veiligheid van bedreigde personen. Daarnaast zijn regels opgenomen over het delen van informatie met andere organisaties, waarbij tegelijkertijd vanuit het oogpunt van gegevensbescherming bepaalde waarborgen zijn opgenomen. Denemarken maakt hiervoor gebruik van één wet, wat op een overzichtelijke manier inzicht geeft in de grondslagen. In andere landen zijn deze grondslagen juist neergelegd in meerdere wetten.

4. Er is een heldere juridische basis voor de inzet van dwangbevoegdheden

De inzet van dwangbevoegdheden kan een grote impact hebben op iemands persoonlijke levenssfeer. Het is daarom van belang dat een heldere juridische basis bestaat, waaruit blijkt wanneer, welke bevoegdheden, door welk orgaan kunnen worden toegepast. Dwangbevoegdheden kunnen nodig zijn om belangrijke informatie te verzamelen, maar dit moet wel op een manier gebeuren waarbij de ingezette bevoegdheid noodzakelijk en proportioneel is.

Een voorbeeld van een land, waarin de dwangbevoegdheden duidelijk in de wet zijn geregeld, is Frankrijk. De mogelijkheden voor organisaties om informatie te verzamelen zijn vastgelegd in de inlichtingenwet. Deze is zowel van toepassing op de inlichtingendiensten als de politie. In wetgeving is tevens geregeld aan welke vereisten geautomatiseerde verwerkingen moeten voldoen en hoe informatie via andere organisaties kan worden verzameld. Frankrijk kent een uitgebreid juridisch kader voor binnenlandse veiligheid, waar specifieke wetgeving (bijvoorbeeld over de bevoegdheden van inlichtingendiensten) aan is toegevoegd. De juridische basis is daarom zowel breed, maar toch gespecialiseerd.

5. De dreigingsanalyse is adequaat/bruikbaar

Voor een goede toegang tot en inzet van het stelsel is een goed bruikbare dreigingsanalyse essentieel. De te nemen maatregelen moeten in verhouding zijn tot het dreigingsniveau. Een te hoog ingeschatte dreigingsanalyse zorgt voor te zware – en dus inefficiënte – inzet van mensen en middelen die mogelijk elders wel (echt) nodig zijn en het maakt tevens een disproportionele inbreuk op de persoonlijke levenssfeer van betrokkene. Een te laag ingeschat dreigingsniveau leidt dan weer tot risico's voor de

veiligheid van betrokkene. Dat betekent dat het dreigingsniveau voldoende nauwkeurig moet kunnen worden ingeschat.

Een voorbeeld dat we hier noemen is Denemarken, vanwege het feit dat informatieverzameling, het opstellen van de dreigingsanalyse en het nemen en uitvoeren van beschermingsmaatregelen onder één dak geregeld is. De PET heeft een sterke informatiepositie en is in beperkte mate afhankelijk van andere organisaties. Dat brengt met zich mee dat het inschatten van het dreigingsniveau gebeurt op basis van de meest actuele beschikbare informatie. Dit verkleint de kans dat er gehandeld wordt op basis van (inmiddels) achterhaalde informatie en dus het risico op een onjuiste dreigingsanalyse.

Een tweede voorbeeld is België. Door een organisatie in het leven te roepen die specifiek gaat over het coördineren van de dreigingsanalyse en het maken van de dreigingsinschatting, komt de informatie van de verschillende betrokken partijen met elk hun eigen expertise (georganiseerde misdaad en terrorisme) op één plek bij elkaar, waardoor het mogelijk wordt een dreigingsbeeld over het geheel te vormen en het dreigingsniveau adequaat in te schatten.

6. De evaluatie van maatregelen is effectief

Periodieke evaluaties van de genomen maatregelen zijn van belang om het maatregelenpakket van een bedreigd persoon aan te laten sluiten bij zijn/haar gewijzigde werkelijkheid. Op basis van nieuwe informatie die in een situatie speelt kunnen maatregelen worden aangescherpt of afgebouwd. Het dilemma dat hierbij speelt is maatregelen na een bepaalde periode geëvalueerd moeten worden om passend te blijven. Anderzijds moeten in uitzonderlijke situaties, wanneer de omstandigheden van een geval hier aanleiding toe geven, maatregelen ook buiten de periodieke evaluatiemomenten kunnen worden aangepast. Het is niet wenselijk dat een casus te vaak geëvalueerd moet worden wanneer een situatie ongewijzigd blijft, om overmatig werk te voorkomen.

In dit kader lichten wij ter illustratie België en Italië uit. In beide landen vindt evaluatie van de maatregelen in ieder geval plaats wanneer er nieuwe informatie beschikbaar is die van belang is voor de beveiligingssituatie van een persoon, bijvoorbeeld wanneer iemand wordt gearresteerd. Daarnaast wordt één keer in de drie maanden (België, Italië) of zes maanden (Italië) de casus van een bedreigde persoon besproken in een overleg. In Italië is sprake van continue monitoring. Dit heeft als voordeel dat een situatie in ieder geval elke 3 of 6 maanden – afhankelijk van het geval – wordt besproken, maar dat ook ingegrepen kan worden wanneer belangrijke nieuwe feiten spelen. Daarvoor hoeft niet gewacht te worden tot het periodieke overleg.

7. Het toezicht is eenduidig en doeltreffend

Het is belangrijk dat betrokken partijen in de uitoefening van hun taken binnen het stelsel van bewaken en beveiligen verantwoording afleggen aan een toezichthoudend orgaan en dat het voor hen duidelijk is aan welk orgaan of welke organen zij dit dienen af te leggen. In het kader van het toezicht speelt bij bewaken en beveiligen het dilemma dat er enerzijds vanwege de gevoelige aard van de werkzaamheden veel informatie niet openbaar kan worden en anderzijds dat een zekere mate van openbaarheid nodig om verantwoording af te kunnen leggen.

Om doeltreffend toezicht op het stelsel mogelijk te maken, lichten wij Frankrijk uit als voorbeeld. Frankrijk heeft in het kader van de Inlichtingenwet ervoor gekozen het toezicht niet te richten op losse onderdelen van het stelsel (zoals toezicht op een bepaalde dienst, of een deelaspect zoals

gegevensbescherming) maar heeft een toezichthouder aangewezen die toezicht houdt op de werking van het gehele stelsel. Hoewel dat in Frankrijk breder is dan het stelsel van bewaken en beveiligen, kan dit wel als inspiratie dienen voor een toezichthouder op dit stelsel. Er is een onafhankelijke commissie ingesteld die adviseert over privacyvraagstukken bij de inzet van instrumenten door inlichtingendiensten. Deze commissie kan voorafgaand, niet-bindend advies uitbrengen aan de premier. Ook kan de commissie achteraf toezicht uitoefenen. Frankrijk heeft wat betreft de balans tussen de vertrouwelijkheid van de werkzaamheden en de mogelijkheid tot verantwoording afleggen, gekozen deze toezichthouder voor het toezicht achteraf permanente, volledige en directe toegang tot dossiers, logs, verzamelde inlichtingen, transcripties en extracties te geven. Tegelijkertijd wordt er in de jaarverslagen niet op casusniveau gerapporteerd zodat deze vertrouwelijk blijven. Het gaat om geaggregeerde data en statistieken.

Een tweede voorbeeld dat wij hier noemen is België. België heeft ervoor gekozen het toezicht op de deelnemende partijen aan het stelsel van bewaken en beveiligen door twee vaste Comités te laten uitoefenen. Door ook het toezicht op gegevensbescherming bij deze vaste Comités te beleggen, is het toezicht niet versnipperd over verschillende toezichthouders op verschillende thema's, maar vallen alle werkzaamheden van de deelnemers onder het toezicht van de Comités.

9. Slotbeschouwing

Om de vragen die centraal staan in dit onderzoek te beantwoorden zijn de onderzoekers in belangrijke mate afhankelijk geweest van de bereidwilligheid van organisaties om de onderzoekers mee te nemen in de vormgeving en werking van het stelsel van bewaken en beveiligen in de onderzochte landen. Dit heeft ertoe geleid dat ten aanzien van vier landen (België, Denemarken, Duitsland (Nedersaksen) en Italië) de verkregen informatie dermate rijk is dat we hebben kunnen komen tot een goede en nuttige vergelijking. Hierdoor hebben we onderzoeksvragen, behoudens onderzoeksvraag 4, kunnen beantwoorden. Om onderzoeksvraag 4 te kunnen beantwoorden waren de onderzoekers afhankelijk van wetenschappers op het vlak van bewaken en beveiligen en daaraan verwante rechtsgebieden. Om verschillende redenen kon daartoe geen medewerking worden verleend.

De onderzoekers constateren dat in de onderzochte landen – bezien in de eigen context en geschiedenis van die landen – verschillende keuzes zijn gemaakt bij het inrichten van het stelsel van bewaken en beveiligen. Deze verschillende smaken bieden kansen voor Nederland om daarvan te leren en inspiratie op te doen, door te bekijken of bepaalde elementen zich lenen om toegepast te worden in het Nederlandse stelsel van bewaken en beveiligen. Wij wijzen daarbij in het bijzonder op de manier waarop de coördinerende rol binnen de verschillende stelsels is ingericht, de wijze waarop casusoverleggen worden gehouden en de wijze waarop dwangbevoegdheden bij wet zijn geregeld.

10. Literatuurlijst

Literatuur

Commissie Bos 2021
Commissie Bos, *Adviescommissie toekomstbestendig stelsel bewaken en beveiligen*, 2021.

Gerards 2023
J.H. Gerards, *General Principles of the European Convention on Human Rights,* Cambrigde University Press 2023.

Gijselaar 2021
E.C. Gijselaar, *Positieve verplichtingen en aansprakelijkheid. De invloed van positieve verplichtingen uit het EVRM op het Nederlandse civiele overheidsaansprakelijkheidsrecht en het materiële strafrecht*, Den Haag: Boom Juridisch 2021.

Gorlé, Bourgeois & Bockert 2007
F.Gorlé, G.Bourgeois & H.Bockert, *Rechtsvergelijking,* Deventer: Wolters Kluwer 2007.

Korten 2015
M.C.P. Korten, *Getuigenbescherming in Nederland* (diss. Rotterdam), Rotterdam: Erasmus Universiteit Rotterdam 2015.

Kranenborg & Verhey 2024
H. R. Kranenborg & L. F. M. Verhey, *De Algemene verordening gegevensbescherming in Europees & Nederlands perspectief*, Deventer: Wolters Kluwer 2024.

NCTV 2025
NCTV, *Dreigingsbeeld Terrorisme Nederland juni 2025*, 2025.

Onderzoeksraad voor Veiligheid 2023
Onderzoeksraad voor Veiligheid, *Bewaken en Beveiligen: Lessen uit drie beveiligingssituaties*, 2023.

Zweigert & Kötz 1998
K. Zweigert & H. Kötz, *An Introduction to Comparative Law,* Oxford: Oxford University Press 1998.

Jurisprudentie
HvJ EU 12 september 2024, ECLI:EU:C:2024:738.

EHRM 7 december 1976, 5493/72 (*Handyside t. Verenigd Koninkrijk*).
EHRM 26 april 1979, 6538/74 (*Sunday Times t. het Verenigd Koninkrijk).*
EHRM 22 oktober 1981, 7525/76 (*Dudgeon t. Verenigd Koninkrijk*).
EHRM 25 juni 1997, 20605/92 (*Halford t. het Verenigd Koninkrijk).*
EHRM 9 juni 1998, 23413/94 (*L.C.B./VK).*
EHRM 28 oktober 1998, 23452/94, (*Osman t het Verenigd Koninkrijk).*
EHRM 28 maart 2000, 22492/93 (*Kılıç t. Turkije*).
EHRM 28 maart 2000, 22535/93 (*Mahmut Kaya t. Turkije*).
EHRM 22 maart 2001, 34044/96, 35532/97, 44801/98 (*Streletz, Kessler and Krenz/Germany).*
EHRM 28 april 2003, 44647/98 (*Peck t. het Verenigd Koninkrijk*).
EHRM 17 oktober 2003, 63737/00 (*Perry t. het Verenigd Koninkrijk).*
EHRM 29 juli 2007*,* 2346/02, (*Pretty t. Verenigd Koninkrijk*).

EHRM 24 september 2007, 5410/03, (*Tysiac t. Polen).*
EHRM 4 december 2008, 30562/04, 30566/04 (*Marper t. het Verenigd Koninkrijk*).
EHRM 9 juni 2009, 33401/02 (*Opuz t. Turkije*).
EHRM 14 september 2010, 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09 (*Dink t. Turkije)*.
EHRM 2 december 2010, 35623/05 (*Uzun t. Duitsland*).
EHRM 10 april 2012, 19986/06 *(Ilbeyi Kemaloğlu & Meriye Kemaloğlu t. Turkije).*
EHRM 16 juni 2015, 64569/09 (*Delfi AS t. Estland).*
EHRM 13 april 2017, 26562/07 (*Tagayeva e.a. t. Rusland).*
EHRM 27 juni 2017, 931/13 (*Satakunnan Markkinapörssi Oy en Satamedia Oy t. Finland*).
EHRM 5 september 2017, 61496/08 (*Barbulescu t. Roemenië*).
EHRM 28 februari 2018, 70838/13 (*Antović en Mirković t. Montenegro*).
EHRM 14 mei 2019, 70573/17 (*Garamukanwa t. het Verenigd Koninkrijk).*
EHRM 15 juni 2021, 62903/15 *(Kurt t. Oostenrijk).*
EHRM 7 maart 2022, 39378/15 (*Standard Verlagsgesellschaft MBH t. Oostenrijk*).
EHRM 7 juli 2022, 72611/14 (*Tagiyeva t. Azerbaijan).*
EHRM 6 juni 2023, 36418/20 (*Navalny t. Rusland no. 3).*
EHRM 20 juni 2023, 36705/16 (*Margari t. Griekenland*).
EHRM 22 juni 2023, 10794/12 (*Giuliano Germano t. Italië*).

Parlementaire stukken
Kamerstukken II 2023/24, 36455, nr. 3.

Tractatenblad
Trb. 1951, 154.
Trb. 1962, 101.
Trb. 1969, 99.
Trb. 1981, 69.
Trb. 1988, 7.
Trb. 2018, 201.
Trb. 2023, 54.

Bronnenlijst gesorteerd op land

België

Literatuur
OCAD 2023
OCAD, *Jaarverslag 2023,* 2023.

Parlementaire stukken
Kamer 2005/06, doc. 51, nr. 2032/001.

Denemarken

Literatuur

Bakker & Vos 2023
E. Bakker & M. Vos, *Reflectie op Bewaken en Beveiligen. vraagstukken en ervaringen in Denemarken, het Verenigd Koninkrijk, Italië en Duitsland*, 2023.

Forsvarsministeriet 2018
Forsvarsministeriet, *Danish Defense Agreement 2018-2023*, 2018.

Graaff e.a. 2018
B. de Graaff e.a., *Handbook of European Intelligence Cultures*, Rowman & Littlefield: Londen 2018.

UNODC 2008
UNODC, *Country Review Report of Denmark,* 2008.

Duitsland

Literatuur

Bakker & Vos 2023
E. Bakker & M. Vos, *Reflectie op Bewaken en Beveiligen. vraagstukken en ervaringen in Denemarken, het Verenigd Koninkrijk, Italië en Duitsland*, 2023.

LKA 2025
LKA, *Organigramm*, 2025.

Rodde 2025
A. Rodde, 'terrorism in France: Overview of the French extremist movements in 2024', *The CRGN Research Notes*, 2025/110.

Frankrijk

literatuur

Tréguer 2021
F. Tréguer, *Overview of France's Intelligence Legal Framework*, Centre de recherches internationales 2021.

Présidence de la République 2025
Présidence de la République, *National Intelligence Strategy. National Intelligence and Counter-Terrorism Coordination*, 2025.

Italië

Literatuur

Bakker & Vos 2023
E. Bakker & M. Vos, *Reflectie op Bewaken en Beveiligen; vraagstukken en ervaringen in Denemarken, het Verenigd Koninkrijk, Italië en Duitsland*, 2023.
Italia dei Valori, *Lo spreco di alcune scorte,* 10 juni 2014.

Peters 2023
L. J. J. Peters, *Hoofdlijnen van de bestrijding van maffiacriminaliteit in Italië. Een verkennende studie voor het debat over de bestrijding van criminele samenwerkingsverbanden in Nederland*, WODC 2023.

Spanje

Literatuur

Ocaña 2013
M. Ocaña, *Prison Conditions in Spain,* European Prison Observatory 2013.

Verenigd Koninkrijk

Literatuur

Hewathanthri 2024
U. Hewathanthri, *Shielding the Vulnerable: A Comparative Study of Victim and Witness Protection in Sri Lanka and the United Kingdom,* 2024.

HMICFRS 2019
HMICFRS, *Police effectiveness, efficiency and legitimacy 2018/19. An inspection of the Metropolitan Police Service,* 2019.

James e.a. 2010
D. V. James e.a., *The Fixated Threat Assessment Centre: preventing harm and facilitating care*, Routledge 2010.

11. Gesprekspartners

Land	Organisatie	Functie
België	Nederlandse ambassade in België	Ambassaderaad Justitie en Veiligheid, Asiel en Migratie
België	Nederlandse ambassade in België	Politie-attaché Nationale Politie voor België en Luxemburg
België	Nederlandse ambassade in België	Assistent Politie attaché
België	DJO	PM
België	NCCN	Permanentiechef bij het Belgisch Nationaal Crisiscentrum
België	OCAD	PM
België	Privaat beveiligingsbedrijf	Directeur
België	Universiteit Gent	Hoogleraar
Denemarken	Justitsministeriet	Fuldmaegtig
Duitsland[248]	Landeskriminalambt Niedersachsen	Kriminaloberkommissar
Frankrijk	Nederlandse ambassade in Frankrijk	Politieattaché
Ierland	Nederlandse ambassade in het Verenigd Koninkrijk	Liaisonmagistraat in het Verenigd Koninkrijk en Ierland
Italië	Nederlandse ambassade in Italië	Liaison
Italië	Nederlandse ambassade in Italië	Liaison assistent
Italië	UCIS	Directrice
Italië	UCIS	Twee medewerkers
Italië		Prefect
Italië	Lumsa Università	Hoogleraar
Italië	Lumsa Università	Hoogleraar
Spanje	Nederlandse ambassade in Spanje	Ambassaderaad Justitie en veiligheid
Spanje	Nederlandse ambassade in Spanje	Politie liaison officer
Spanje	Unidad Central de Protección, Policia National	Jefa de Sección operativa de dispositivos especiales
Spanje	Universidad Zaragoza	Hoogleraar
Verenigd Koninkrijk	Nederlandse Ambassade in het Verenigd Koninkrijk	Ambassaderaad voor justitie
Verenigd Koninkrijk	Nederlandse Ambassade in het Verenigd Koninkrijk	Liaisonmagistraat in het Verenigd Koninkrijk en Ierland

[248] Schriftelijk toegestuurde informatie.

HOOGHIEMSTRA & PARTNERS

strategisch en juridisch advies

Bezuidenhoutseweg 161, 2594 AG Den Haag • **T** +31 (0) 6 39 27 85 33
E info@hooghiemstra-en-partners.nl • www.hooghiemstra-en-partners.nl
ING Bank NL49INGB0008938076 • **KvK** 73390356 • **BTW** 8595.06.447.B01