nationale ombudsman

Blind vertrouwen?

Een onderzoek naar CTER-registraties en de impact ervan op het leven van burgers

Rapportnummer: 2024/098 | Datum: 12 november 2024

Onderzoeksteam
Chloë van Vliet, projectleider
Silvija Andric, onderzoeker
Jochem Blad, onderzoeker
Ilse de Jong, projectsecretaris
Ailie Tio, onderzoeker
Christine Tromp, onderzoeker
Janneke van Veen, senior-onderzoeker
Ayeh Zarrinkhameh, senior-onderzoeker

Laura van den Heuvel, hoofd onderzoek

Datum: 12 november 2024
Rapportnr: 2024/098

Inhoudsopgave

Beschouwing

Wanneer ik als Nationale ombudsman een klacht ontvang, dan doe ik wat mogelijk is om een oplossing te vinden voor het probleem waar de burger tegenaan loopt. Als meerdere mensen mij met hetzelfde probleem benaderen, dan is dat voor mij aanleiding om eens goed te bekijken wat er nu precies achter deze klachten schuilgaat. Dat was het geval bij klachten over registraties die te maken hebben met Contraterrorisme, Extremisme en Radicalisering (CTER-registraties). Burgers vertelden mij dat ze onverwachts in de problemen kwamen en bijvoorbeeld een ander land niet in mochten, vragen kregen aan de grens of zelfs werden vastgezet. In alle gevallen tastten ze in het duister over de oorzaak. Dat beeld, dat een burger zo machteloos staat tegenover de overheid, liet mij niet los.

De samenleving mag van de overheid verwachten dat zij zorgt voor veiligheid en burgers beschermt tegen de dreiging die uitgaat van extremistische en geradicaliseerde individuen. Dat is belangrijk, want onze veiligheid is een groot goed. Een actieve overheid beschermt de nationale veiligheid. Zij doet dat in samenwerking met andere overheden in en buiten de Europese Unie. De ervaringen van de burgers die zich tot mij hebben gewend, tonen echter de keerzijde van deze medaille. Hun gegevens worden geregistreerd, besproken en gedeeld, zonder dat duidelijk is waarom, wie dit heeft gedaan en hoe de betrokkenen een eventueel onterechte registratie kunnen aanvechten. Dit raakt aan hun individuele rechten en vrijheden en heeft daarmee impact op hun leven.

Deze ervaringen kon ik als Nationale ombudsman niet negeren. Daarom ben ik een onderzoek gestart: om te zien of de overheid op een behoorlijke manier omgaat met de gegevens van burgers. Ik wilde weten in hoeverre het CTER-proces rekening houdt met de belangen van burgers die in de gaten worden gehouden. Want het werd me duidelijk dat dat proces aan de basis kan liggen van maatregelen waar burgers last van kunnen hebben. Ook wilde ik weten of de betrokken overheidsinstanties het perspectief van de burger meewegen in de beslissingen die ze nemen. Het is namelijk van belang dat je erop kunt vertrouwen dat de overheid goed omgaat met je gegevens, belangen en rechten – zeker wanneer je gegevens worden verwerkt zonder jouw medeweten.

Het rapport dat voor u ligt is het resultaat van dit onderzoek. Ik roep alle betrokkenen op om de conclusies ter harte te nemen en de burger centraal te stellen bij het verder verbeteren van het CTER-proces.

Den Haag, 12 november 2024

De Nationale ombudsman,
Reinier van Zutphen

Samenvatting

Aanleiding onderzoek
Extremisme en radicalisering kunnen risico's met zich meebrengen voor de samenleving. Daarom hebben Europese overheden – waaronder de Nederlandse – wettelijke bevoegdheden en systemen in het leven geroepen. Een onderdeel van de Nederlandse aanpak vormen de vroegsignalering en registratie van burgers die mogelijk een dreiging (gaan) vormen. In Nederland worden deze registraties *CTER-registraties* genoemd. CTER staat voor Contraterrorisme, Extremisme en Radicalisering. De overheid hoopt met deze registraties en met mogelijk daaruit voortvloeiende signaleringen (potentieel) extremistische en/of geradicaliseerde burgers dusdanig goed in de gaten te kunnen houden, dat terroristische aanslagen worden voorkomen. De CTER-registraties en signaleringen van burgers – die veelal niet worden verdacht van of zijn veroordeeld voor een strafbaar feit – staan echter op gespannen voet met de individuele rechten en vrijheden van die burgers.

De Nationale ombudsman heeft meerdere klachten en signalen ontvangen van en over burgers die problemen hebben ondervonden waarvan ze vermoeden dat die te maken hebben met een CTER-registratie. Hun ervaringen waren voor de Nationale ombudsman aanleiding tot zorgen over de CTER-registraties en signaleringen. Die zorgen gaan over de vraag of de overheid behoorlijk handelt, vanaf de CTER-registratie tot aan het moment dat burgers in de problemen komen en zich tot de overheid wenden met vragen. Vanwege deze zorgen heeft de Nationale ombudsman besloten op 19 februari 2024 een onderzoek te starten.

Doel- en vraagstelling
De Nationale ombudsman wil bijdragen aan een behoorlijke behandeling van burgers in het CTER-proces, vanaf het moment van registratie tot en met het signaleren van burgers in internationale informatiesystemen. En wanneer burgers om opheldering vragen omdat ze tegen problemen aanlopen en/of zaken willen rechtzetten. De Nationale ombudsman onderzoekt daarom of de overheid het burgerperspectief voldoende waarborgt. De hoofdvraag van dit onderzoek luidt daarom als volgt:

Behandelt de Nederlandse overheid burgers met een CTER-registratie behoorlijk?

Aanpak
Om inzicht te krijgen in de problematiek heeft de Nationale ombudsman gesproken met burgers, advocaten, wetenschappers, belangenorganisaties en een journalist. Daarnaast heeft de Nationale ombudsman gesprekken gevoerd met de Nationale Politie, de Koninklijke Marechaussee (KMar), het Openbaar Ministerie (OM), het ministerie van Justitie en Veiligheid (ministerie van JenV), het ministerie van Buitenlandse Zaken (ministerie van BZ), de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), de Autoriteit Persoonsgegevens (AP), de Inspectie Justitie en Veiligheid (Inspectie JenV) en met de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Tot slot heeft de Nationale ombudsman kennisgenomen van relevante wet- en regelgeving, beleidsdocumenten en Kamerstukken.

Conclusies onderzoek

CTER-proces is complex en ondoorzichtig voor burgers
Voor burgers is het systeem rondom CTER-registraties ondoorgrondelijk; een black box. Burgers weten over het algemeen niet dát ze in beeld zijn en met welke instanties en/of landen informatie over hen wordt gedeeld. De gevolgen kunnen echter groot zijn. Daardoor komt hun recht op privacy onder druk te staan, zonder dat ze daar iets van merken. Burgers weten pas dat er iets aan de hand is als ze in hun dagelijks leven tegen de gevolgen aanlopen. Ze weten niet wat de oorzaak is en waar ze moeten beginnen met zoeken om daarover duidelijkheid te krijgen. Er kunnen veel verschillende instanties in binnen- en buitenland bij betrokken zijn.

Te veel nadruk op veiligheidsdenken vormt risico
Het CTER-proces kent waarborgen om te voorkomen dat burgers zomaar op een lijst terechtkomen. Er bestaat echter een risico dat er in het CTER-proces te veel nadruk ligt op het veiligheidsdenken, terwijl er sprake moet zijn van een balans tussen de nationale veiligheid aan de ene kant en individuele mensenrechten aan de andere kant. Het besef dat de afwegingen en keuzes in het CTER-proces grote impact kunnen hebben op de individuele rechten en vrijheden van burgers kan makkelijk op de achtergrond raken doordat de nationale veiligheid prioriteit heeft.

Toezicht onvoldoende structureel ingevuld
Structureel en onafhankelijk toezicht op het CTER-proces is op dit moment te mager georganiseerd. Het proces ontbeert een structurele blik van buiten. Burgers moeten erop kunnen vertrouwen dat de overheid goed omgaat met hun gegevens, belangen en rechten. Onafhankelijk en structureel toezicht is daarvoor een belangrijke voorwaarde. Dat is des te belangrijker als burgers geen weet hebben van de verwerking van hun gegevens, zoals bij CTER-registraties, en deze verwerking bovendien grote gevolgen kan hebben voor hun leven en dat van hun familie.

Rechtsbescherming is niet effectief voor de burger
De beslissingen en afwegingen van de betrokken instanties moeten navolgbaar, uitlegbaar en controleerbaar zijn. Burgers hebben een aantal middelen om te achterhalen en controleren wat de overheid over hen heeft vastgelegd en gedeeld. Dat begint meestal met een inzageverzoek. Inzageverzoeken geven echter vaak geen volledig beeld van wat er over hen is vastgelegd en gedeeld en waarom. Ook krijgen burgers in de praktijk geen antwoord op de vraag of een eventuele gegevensdeling of signalering terecht en proportioneel was. Als inzageverzoeken geen duidelijkheid bieden, dan kunnen burgers in beroep gaan bij de rechter of naar de AP gaan voor bemiddeling of een klachtenprocedure. Burgers benutten de mogelijkheden bij de AP echter nauwelijks, omdat deze procedures voor hen niet voldoende bekend zijn. Hoewel burgers vaker kiezen voor de weg naar de rechter, levert een juridische procedure vaak evenmin duidelijkheid op.

Aanbeveling
De Nationale ombudsman vindt dat het beter kan en beter moet. Daarom beveelt hij de minister van Justitie en Veiligheid aan om, samen met de betrokken instanties, de genoemde tekortkomingen aan te pakken. En concrete verbeteringen te verwezenlijken op de door de ombudsman genoemde knelpunten. Alleen dan kunnen burgers erop vertrouwen dat hun individuele rechten en vrijheden niet naar de achtergrond verdwijnen bij het beschermen van de nationale veiligheid.

1 Inleiding

1.1 Aanleiding van het onderzoek

Extremisme en radicalisering kunnen risico's met zich meebrengen voor de samenleving. Daarom hebben Europese overheden – waaronder de Nederlandse – wettelijke bevoegdheden en systemen in het leven geroepen. Een onderdeel van de Nederlandse aanpak vormen de vroegsignalering en registratie van burgers die mogelijk een dreiging (gaan) vormen.[1] In Nederland worden deze registraties *CTER-registraties* genoemd. CTER staat voor Contraterrorisme, Extremisme en Radicalisering. De politie en de KMar kunnen dergelijke registraties aanmaken door een CTER-projectcode te koppelen aan een gebeurtenis. Als hiertoe aanleiding is, kunnen de politie en de KMar de betrokken burgers – na duiding van de gebeurtenis – opnemen in het zogenoemde *themaregister CTER*.[2] Op dat moment zijn ze in beeld bij de autoriteiten. In afstemming met het bevoegd gezag – het OM – kan besloten worden tot nadere maatregelen, zoals een internationale signalering. Daarbij hoeft er geen sprake te zijn van een verdenking in strafrechtelijke zin, dus geen redelijk vermoeden van een strafbaar feit. Een aanwijzing van een terroristisch misdrijf is voldoende. De overheid hoopt met deze registraties en met mogelijk daaruit voortvloeiende signaleringen (potentieel) extremistische en/of geradicaliseerde burgers dusdanig goed in de gaten te kunnen houden, dat terroristische aanslagen worden voorkomen.

De CTER-registraties en signaleringen van burgers – die veelal niet worden verdacht van of zijn veroordeeld voor een strafbaar feit – staan echter op gespannen voet met de individuele rechten en vrijheden van die burgers. Een maatregel, zoals een signalering, kan ertoe leiden dat ze problemen ondervinden in het dagelijks leven, zonder te weten waarom. Burgers weten niet altijd dát ze in beeld zijn en met welke instanties of met welke andere landen informatie over hen is gedeeld.

Klachten

De Nationale ombudsman heeft meerdere klachten en signalen ontvangen van en over burgers die problemen hebben ondervonden waarvan ze vermoeden dat die te maken hebben met een CTER-registratie. Sommigen van hen mochten bijvoorbeeld op vakantie onverwacht het land van bestemming niet in of zijn zelfs aan de grens in detentie genomen. In een aantal gevallen bleek naderhand dat de problemen CTER-gerelateerd waren; in andere gevallen is de aanleiding onduidelijk gebleven. De ervaringen van deze burgers komen aan de orde in hoofdstuk 2 en geven een indruk van de problemen waar ze tegenaan lopen en de impact hiervan op hun leven.

Uit de klachten blijkt dat het voor burgers moeilijk is om via de reguliere procedures zicht te krijgen op wat er over hen in welke overheidssystemen staat en waarom. Het is evenmin duidelijk wat ze moeten doen als ze dat willen laten corrigeren. Burgers vragen zich af welke afwegingen aan deze registratie ten grondslag liggen en waarom er informatie over hen is gedeeld. Het lukt hun niet om een duidelijk antwoord te krijgen op al deze vragen. Daarom hebben verschillende van deze burgers bij de ombudsman aangeklopt. De ombudsman ziet echter dat individuele klachtbehandeling op grond van de Algemene wet bestuursrecht (Awb) veelal geen oplossing zal bieden voor deze burgers. Dat heeft verschillende redenen. Zo is veel informatie afgeschermd (vanwege de nationale veiligheid). De ombudsman kan de informatie wel inzien, maar mag die niet delen met burgers. Daarnaast kan de oorzaak van de problemen

[1] Een beschrijving van de bredere contraterrorismestrategie is te vinden in de Nationale Contraterrorisme Strategie 2022-2026.
[2] Op grond van artikel 10,1b Wpg kan de politie themaregisters gebruiken om inzicht te krijgen in de betrokkenheid van personen bij bepaalde ernstige misdrijven, zoals mensenhandel en terrorisme. Dit wordt verder toegelicht in paragraaf 4.3.

ook in het buitenland liggen of bij de (Nederlandse of buitenlandse) inlichtingen- en veiligheidsdiensten. Daarover is de ombudsman niet bevoegd en de ombudsman kan deze informatie dan ook niet achterhalen. Verder ligt de nadruk in het CTER-proces op gegevensverwerkingen en -delingen, en dat is het terrein van de AP en daarna eventueel van de bestuursrechter. De AP beschikt over vergaande bevoegdheden op het gebied van de naleving van regels voor de bescherming van persoonsgegevens.

Onderzoek
De klachten en signalen van burgers waren voor de Nationale ombudsman aanleiding tot zorgen over de CTER-registraties en signaleringen. Onderzoekers van de ombudsman zijn daarom over dit onderwerp in gesprek gegaan met onder meer de politie en wetenschappers en advocaten die zich met deze problematiek bezighouden. Deze gesprekken vergrootten de zorgen van de ombudsman. Daarom heeft de Nationale ombudsman besloten op 19 februari 2024 een onderzoek te starten naar CTER-registraties en signaleringen.

1.2 Afbakening van het onderzoek

Het onderzoek van de Nationale ombudsman richt zich op een onderdeel van de bredere contraterrorismestrategie, namelijk de CTER-registraties door de politie[3] en de KMar[4], signaleringen of gegevensdelingen en de gevolgen daarvan. In het onderzoek brengen we dit onderdeel van de contraterrorismeaanpak in Nederland in kaart, zoals die nu is vormgegeven. Zoals hierboven vermeld, kan de ombudsman burgers via individuele klachtbehandeling veelal niet bieden waar ze naar op zoek zijn. Daarom richten we ons op het proces: we willen nagaan of het huidige proces zo is ingericht dat burgers erop kunnen vertrouwen dat beslissingen zorgvuldig worden genomen. En of hun rechten daarin voldoende zijn beschermd door waarborgen in het proces en door onafhankelijk toezicht. Het onderzoek richt zich specifiek op de groep burgers die (mogelijk) een CTER-registratie op hun naam hebben en veelal niet zijn aangemerkt als verdachte in strafrechtelijke zin. Deze burgers hebben niet de rechten die horen bij de status van verdachte en weten daarom ook niet dat zij in beeld zijn en waarom.

Onze focus op het huidige proces betekent dat we niet naar het proces hebben gekeken zoals dat in het verleden was ingericht. Het kan zijn dat problemen die burgers ondervinden, zijn veroorzaakt door een werkwijze die in het verleden werd gehanteerd. Maar ook binnen de huidige werkwijze kunnen er beslissingen worden genomen met een vergelijkbare impact.

De onderzoekers hebben niet bekeken hoe andere landen omgaan met informatie die afkomstig is van Nederlandse autoriteiten en welke waarborgen er in die landen gelden. Daartoe is de ombudsman niet bevoegd. Ook geeft de ombudsman geen oordeel over de manier waarop de Nederlandse overheid haar zorgplicht invult voor burgers die in het buitenland in de problemen komen. De overweging hierbij was dat het onderzoek daarmee te groot en complex zou zijn geworden.

Voor de volledigheid merken we op dat de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) buiten dit onderzoek valt. De AIVD vervult weliswaar een grote rol in de uitvoering van de contraterrorismestrategie en kan ook mensen laten signaleren, maar de ombudsman is niet bevoegd als het gaat om klachtbehandeling door en toezicht op de AIVD. Die bevoegdheid ligt bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Het kan wel

[3] Artikel 3 van de Politiewet 2012 omschrijft de taak van de politie als volgt: 'De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.'
[4] De KMar is onderdeel van het Ministerie van Defensie en voert politietaken uit op grond van de Politiewet (zie artikel 4). De hoofdtaken zijn: grenspolitietaak, bewaken en beveiligen en (inter)nationale en militaire politie(zorg)taken.

zo zijn dat de problemen die burgers beschrijven (mede) hun oorsprong hebben in het handelen van de AIVD.

In dit onderzoek worden de termen *CTER-proces*, *CTER-registratie*, *CTER-projectcode* en *signalering* gebruikt:

- CTER-proces: het proces van de verwerking van politiegegevens dat de betrokken instanties hebben ingericht in het kader van contraterrorisme, extremisme en radicalisering.
- CTER-registratie: een CTER-gerelateerde gegevensverwerking in algemene zin (zoals geregistreerd door de politie of de KMar).
- CTER-projectcode: een codering van een mogelijk CTER-gerelateerde gebeurtenis, zodat deze gebeurtenis nader kan worden geduid.
- signalering: het signaleren van burgers in (internationale) informatiesystemen, zoals het Schengen Informatie Systeem (SIS), of via Interpol. Een signalering bevat informatie over een specifieke persoon of een specifiek voorwerp en instructies voor de autoriteiten over wat die moeten doen wanneer die persoon of dat voorwerp is gevonden.

In hoofdstuk 4 staat het CTER-proces nader beschreven. Daar komen ook de verschillende termen aan de orde.

1.3 Doel- en vraagstelling

De hoofdvraag van dit onderzoek luidt als volgt:

Behandelt de Nederlandse overheid burgers met een CTER-registratie behoorlijk?

Om de hoofdvraag te kunnen beantwoorden, stellen we de volgende deelvragen:

- Waar lopen burgers tegenaan in relatie tot het CTER-proces?
- Hoe ziet het CTER-proces eruit in de praktijk, vanaf de CTER-registratie tot signalering?
- Waar kunnen burgers terecht als ze vermoeden dat er een CTER-registratie of signalering op hun naam staat?
- Wat kunnen burgers doen tegen een CTER-registratie (of de gevolgen daarvan)?
- Welke rechtsbescherming kent het CTER-proces?
- Hoe is het toezicht op het CTER-proces geregeld?
- Hoe kijkt de overheid naar het perspectief van burgers?

Het doel van het onderzoek is bij te dragen aan een behoorlijke behandeling van burgers in het CTER-proces, vanaf de CTER-registratie tot en met het signaleren van burgers in internationale informatiesystemen, en wanneer burgers om opheldering vragen omdat ze tegen problemen aanlopen en/of zaken willen rechtzetten. De Nationale ombudsman onderzoekt daarom of de overheid het burgerperspectief voldoende waarborgt.

1.4 Aanpak

Om inzicht te krijgen in de problematiek heeft de Nationale ombudsman gesproken met burgers die zich hebben gemeld met klachten of signalen, en ook met advocaten, wetenschappers, belangenorganisaties en een journalist die zich met deze problematiek bezighouden. Daarnaast voerde de ombudsman gesprekken met overheidsinstanties die een rol hebben in het proces van CTER-registraties en signaleringen: de Nationale Politie, de KMar, het OM en het ministerie van JenV. De ombudsman sprak ook met toezichthoudende overheidsinstanties, zoals de AP en de Inspectie JenV, en met de CTIVD, omdat die, net als de AP, toezicht houdt op instanties die

(gevoelige) persoonsgegevens verwerken. Verder waren er gesprekken met het ministerie van BZ en de NCTV. Tot slot heeft de ombudsman kennisgenomen van relevante wet- en regelgeving, beleidsdocumenten en Kamerstukken.

In bijlage 1 staat een uitgebreidere beschrijving van de aanpak van het onderzoek.

1.5 Leeswijzer

In hoofdstuk 2 beginnen we met het burgerperspectief: wat mogen burgers van de overheid verwachten als het gaat om het CTER-proces? Vervolgens beschrijven we de ervaringen van mensen die in het CTER-proces betrokken (denken te) zijn geraakt, zoals zijzelf of hun vertegenwoordigers aan ons hebben verteld. We laten zien waar deze burgers tegenaan zijn gelopen en hoe zij het contact daarover met de overheid hebben ervaren. We benoemen daarbij ook welke mensenrechten er in het geding zijn.

De visie van de betrokken overheidsinstanties op de problematiek volgt in hoofdstuk 3. In hoofdstuk 4 beschrijven we het CTER-proces bij de politie en de KMar en de maatregelen die zij in dat kader kunnen nemen, in samenspraak met het OM. Inzage, toezicht en rechtsbescherming komen aan de orde in hoofdstuk 5. In hoofdstuk 6 staan de conclusies uit ons onderzoek en een aanbeveling voor de minister van JenV. In de bijlagen geven we een toelichting op de aanpak van het onderzoek, gevolgd door een overzicht van het juridisch kader van de gegevensverwerking in het CTER-proces en een afkortingenlijst.

In het rapport staan citaten weergegeven die de verschillende perspectieven illustreren van de mensen die de Nationale ombudsman in het kader van dit onderzoek heeft gesproken.

2 Burgerperspectief en ervaringen van burgers

2.1 Inleiding

De Nationale ombudsman beschrijft in dit hoofdstuk de ervaringen van burgers die mogelijk te maken hebben (gehad) met een CTER-registratie. Deze burgers hebben verteld waar ze tegenaan lopen en wat er beter zou kunnen. Om dit in perspectief te plaatsen en concreet te maken wat burgers van de overheid mogen verwachten, beschrijven we hier eerst het burgerperspectief.

2.2 Burgerperspectief: wat mogen burgers van de overheid verwachten?

Zoals uitgelegd in de inleiding en zoals blijkt uit de ervaringen van burgers, die verderop aan de orde komen, kunnen de bevoegdheden van de overheid op het gebied van CTER-registraties en signaleringen diep ingrijpen op het leven van burgers. Deze bevoegdheden gebruikt de overheid als onderdeel van haar taak om de nationale veiligheid te beschermen, maar deze kunnen op gespannen voet staan met de individuele rechten en vrijheden van burgers. Het is aan de overheid om ervoor te zorgen dat die rechten en vrijheden worden gewaarborgd.

Klassieke mensenrechten zijn er om het individu te beschermen tegen de macht van de staat. Die mag deze rechten alleen inperken als de wet dat expliciet toestaat, dit een legitiem doel dient en noodzakelijk is in een (democratische) samenleving.[5] De rechten van het individu moeten worden afgewogen tegen het algemeen belang. Daarmee kunnen verschillende belangen worden bedoeld, bijvoorbeeld het belang van de bescherming van de rechten en vrijheden van anderen, de bescherming van de gezondheid, of het economisch welzijn van het land. Ook de nationale veiligheid kan een belang zijn om de rechten van individuele burgers in te perken.[6] In de verderop beschreven verhalen van burgers maken we waar mogelijk een koppeling met de mensenrechten die onder druk kunnen komen te staan. Het gaat dan om het recht op privacy en de bescherming van persoonsgegevens, het recht op bewegingsvrijheid, het recht op behoud van familie- of gezinsleven en het recht op rechtsbescherming.

Ook bij de inrichting en uitvoering van het CTER-proces is de overheid verantwoordelijk voor het waarborgen van de mensenrechten. Het is begrijpelijk dat de overheid, zowel tijdens het CTER-proces als achteraf, niet altijd openheid kan geven over haar beslissingen en de afwegingen die eraan ten grondslag liggen. Burgers krijgen daar dus vaak weinig informatie over. Daarom is het belangrijk dat het proces dermate zorgvuldig verloopt dat burgers erop kunnen vertrouwen dat de overheid hun rechten respecteert. Alleen dan is het acceptabel dat de rechten van individuele burgers beperkt worden met het oog op de nationale veiligheid.

Wat betekent dit concreet? Wat mogen burgers van de overheid verwachten als ze in het CTER-proces betrokken raken?

- De overheid moet zorgen voor waarborgen die garanderen dat het vastleggen of delen van gegevens proportioneel is en niet onnodig ingrijpt in het leven van burgers. De beslissingen en afwegingen rond de registratie en het delen van gegevens moeten worden vastgelegd, zodat ze later inzichtelijk en toetsbaar zijn. De overheid moet zich realiseren dat CTER-registraties en signaleringen een inbreuk kunnen vormen op mensenrechten.

[5] Dit laatste vereiste valt uiteen in vier elementen: er moet sprake zijn van een *pressing social need* (1), de maatregel moet geschikt zijn om het legitieme doel te bereiken (2) en de beperking moet proportioneel (3) en subsidiair (4) zijn.
[6] Het begrip nationale veiligheid kent in Europese regelgeving overigens geen eenduidige definitie, maar omvat volgens het Europees Hof voor de Rechten van de Mens (EHRM) in ieder geval de bescherming van de veiligheid van de staat en de democratische rechtsorde tegen terrorisme.

- De overheid moet structureel en onafhankelijk toezicht organiseren in alle fasen van het proces. Er moet een blik van buiten zijn die het functioneren van de waarborgen kan controleren en waar nodig kan bijsturen. De toezichthouder moet ook openbaar over de bevindingen rapporteren.

- De overheid moet zorgen voor effectieve en voor burgers vindbare mogelijkheden om de betrokken instanties om duidelijkheid en, waar mogelijk, een oplossing te vragen. Dat betekent overigens niet dat burgers zélf altijd alle informatie moeten kunnen inzien. Wel moeten ze de mogelijkheid hebben om de afwegingen die in hun geval zijn gemaakt, te laten toetsen.

De ombudsman vindt dat de overheid dit burgerperspectief als uitgangspunt moet nemen bij het inrichten van haar processen. Op basis van de ervaringen van burgers en overheidsinstanties en de beschrijving van het huidige CTER-proces bekijken we in hoeverre het burgerperspectief is gewaarborgd in het handelen van de politie, de KMar en het OM.

2.3 Wat burgers ons vertelden

In deze paragraaf beschrijven we de klachten waarmee burgers zich tot de Nationale ombudsman hebben gewend. Dit zijn – logischerwijs – burgers die op enig moment zelf hebben gemerkt dat ze (extra) gevolgd of gecontroleerd werden. Zij deden bij de ombudsman hun verhaal over de praktische problemen waar ze tegenaan liepen en soms nog steeds lopen, en vertelden ook hoe het voelde om op die manier benaderd te worden. Verder schetsten ze hun – vaak vergeefse – zoektocht naar de reden van de problemen waar ze mee te maken kregen. Aan de hand van citaten uit hun berichten en onze gesprekken met hen laten we zien wat hun ervaringen zijn.[7] Daarbij beschrijven we ook wat advocaten, belangenbehartigers, wetenschappers en een journalist vertelden over de problemen waar deze burgers tegenaan lopen.

De meeste burgers vermoeden dat een CTER-registratie hun problemen veroorzaakt, maar hebben dit niet kunnen vaststellen. Deze paragraaf toont dus de ervaringen van burgers die vermoeden via een CTER-registratie in beeld te zijn bij de Nederlandse en/of buitenlandse autoriteiten. Of het ook daadwerkelijk om CTER-registraties gaat en in hoeverre de politie, de KMar en het OM hierbij betrokken zijn, is niet altijd duidelijk.

Omdat CTER-projectcodes achter de schermen worden geregistreerd en beoordeeld, zijn burgers in principe niet op de hoogte van het feit dat ze in beeld zijn. Toch staan hun rechten en vrijheden op het spel op het moment dat instanties informatie over hen verwerken, opvragen en bespreken en die informatie onderling uitwisselen. Ook als ze daar zelf niets van merken. Normaal gesproken blijven burgers gevrijwaard van dergelijke overheidsbemoeienis en zijn ze vrij in hun doen en laten, zolang ze daarbij de wet niet overtreden. Bij burgers die een CTER-registratie hebben, kan het zo zijn dat ze de wet niet overtreden, geen verdachte zijn en niet vervolgd worden voor enig strafbaar feit, maar toch in de gaten worden gehouden omdat ze volgens de instanties mogelijk een dreiging (gaan) vormen. Vaak duurt dat maar kort, maar soms gaat het om een langere periode. Als de politie er reden toe ziet, kan zij in overleg met het OM besluiten om maatregelen te nemen die, afhankelijk van de maatregel, al dan niet voor burgers zelf merkbaar zijn.

Het is niet duidelijk hoe groot de groep burgers is die problemen ondervindt. Media berichten over tientallen Nederlanders die op buitenlandse luchthavens worden teruggestuurd of vast

[7] Het ministerie van JenV heeft aangegeven niet te kunnen ingaan op de individuele zaken die we in dit hoofdstuk hebben beschreven, ook als het vindt dat er feitelijke onjuistheden in staan.

komen te zitten vanwege terrorismerisico's, terwijl ze zelf in het duister tasten over de achtergrond van die verdenkingen.[8] De partijen waarmee de ombudsman gesprekken heeft gevoerd, denken dat de werkelijke omvang groter is dan nu zichtbaar is. Zij geven aan dat veel mensen zich niet melden, omdat ze niet met de overheid in contact willen zijn over iets wat verband houdt met terrorisme.

Een journalist benoemt daarnaast dat het niet uitmaakt hoe groot de groep is.

> **Journalist:** 'Ook als dit bij 100 mensen zou spelen: het gaat om individuele burgers en een fundamenteel probleem. Dan hoeft de ernst niet van de aantallen af te hangen.'

Lage lat voor registratie

Volgens de juridische professionals die de Nationale ombudsman heeft gesproken, ligt de lat voor registratie van burgers laag en zijn de uiteindelijke (potentiële) gevolgen voor de betrokkene groot. Een advocaat stelde dat ze de indruk heeft dat kleine dingen al een CTER-registratie kunnen opleveren, bijvoorbeeld een 'verkeerde blik', een lange baard, deelname aan een demonstratie of een contactmoment met iemand die een CTER-registratie heeft. Waarom burgers een CTER-registratie op hun naam krijgen, is voor hen vaak niet goed te achterhalen, zoals hierboven al aan de orde kwam. Een deel van de geïnterviewde burgers weet niet hoe ze de aandacht van de autoriteiten op zich gevestigd hebben gekregen. Toen aan hen werd gevraagd welke ideeën ze daar zelf over hebben, kwamen ze met verschillende vermoedens. Eén burger, die zich inzet tegen racisme en voor vluchtelingen denkt dat hij in beeld is gekomen vanwege zijn contacten met burgers met een CTER-registratie, maar gaf aan zelf nooit verdachte te zijn geweest of ergens voor te zijn veroordeeld. Een andere burger vertelde dat de politie vragen had omdat hij een moskee bezocht waar ook 'radicale' jongeren kwamen die hij zou kennen. Een belangenorganisatie zei dat slechts in enkele van de zaken die zij kennen sprake is van iemand die ook daadwerkelijk verdachte is geweest. Deze organisatie stelt dat de overige personen vermoedelijk op een lijst zijn gekomen omdat ze contact met iemand hebben gehad. Je bent blijkbaar al interessant als je in contact bent met een verdacht persoon, aldus de belangenorganisatie.

Burgers en advocaten menen dus dat er weinig bijzonders voor nodig is om in beeld te komen, terwijl de gevolgen groot kunnen zijn. Zodra mensen merken dat ze gevolgd worden, ervaren ze een beperking in hun bewegingsvrijheid,[9] een verminderd gevoel van veiligheid en vertrouwen in de overheid en een schending van hun privacy. Daaruit blijkt dat hun recht op bewegingsvrijheid en hun recht op privacy in het geding kunnen komen.

> **Burger:** 'Het is beangstigend hoe het nu gaat. Het is schadelijk en leidt tot onzekerheid.'

[8] Zie het artikel van Follow the Money van 6 mei 2023, 'Op de Amerikaanse terroristenlijst, zonder te weten waarom'.
[9] Zie artikel 12 Internationaal verdrag inzake burgerrechten en politieke rechten: '1. Een ieder die wettig op het grondgebied van een Staat verblijft, heeft, binnen dit grondgebied, het recht zich vrijelijk te verplaatsen en er zijn verblijfplaats vrijelijk te kiezen. 2. Een ieder heeft het recht welk land ook, met inbegrip van het eigen land, te verlaten. 3. De bovengenoemde rechten kunnen aan geen andere beperkingen worden onderworpen dan die welke bij de wet zijn voorzien, nodig zijn ter bescherming van de nationale veiligheid, de openbare orde, de volksgezondheid of de goede zeden of van de rechten en vrijheden van anderen en verenigbaar zijn met de andere in dit Verdrag erkende rechten. 4. Aan niemand mag willekeurig het recht worden ontnomen naar zijn eigen land terug te keren.' Zie ook artikel 2 van het Vierde protocol bij het Europees Verdrag voor de Rechten van de Mens (EVRM) en artikel 45 Handvest grondrechten van de EU.

Advocaten vinden dat er in algemene zin te weinig is nagedacht over de proportionaliteit van alle stappen, vanaf de CTER-registratie tot het signaleren en andere maatregelen die de instanties kunnen nemen. Advocaten vinden dat deze stappen te lichtvaardig en zonder goede waarborgen worden gezet. Mensen die in beeld zijn bij overheidsinstanties in verband met terrorisme, komen daar maar moeilijk vanaf, zo geven ze aan. Het recht op bescherming van persoonsgegevens kan hierdoor onder druk komen te staan.[10]

Problemen met reizen naar het buitenland
De meeste burgers die de ombudsman heeft gesproken, kwamen er bij het reizen naar het buitenland achter dat er iets aan de hand was, of hadden dat vermoeden. Ze kregen bijvoorbeeld geen visum voor een bepaald land. Ook vertelden burgers dat ze bij elke reis opnieuw aan de grens werden ondervraagd als ze een ander land binnen wilden. Soms werden ze, zonder dat ze enig idee hadden van de aanleiding, meegenomen naar een aparte ruimte en daar ondervraagd. Meerdere personen kregen aan de grens met een ander land bijvoorbeeld heel specifieke vragen over radicalisering, ISIS en terrorisme. Eén burger gaf aan dat hij werd meegenomen naar een kantoor en daar door vijf personen werd ondervraagd.

De mensen die aan de grens werden ondervraagd mochten in sommige gevallen daarna alsnog het betreffende land in. Maar het kwam ook regelmatig voor dat hun de toegang tot het land werd geweigerd, waardoor hun reis niet kon doorgaan. In enkele gevallen werd een burger zelfs vastgezet in de cel, soms voor meerdere dagen. Terwijl het voor die persoon al die tijd niet duidelijk was wat hiervoor de reden was.

Burger: ‘Bij aankomst in Antalya werd de toegang van alleen mij geweigerd. Ze hebben mij een dag vastgehouden in een cel en zeiden dat er een ban op mijn naam staat die betrekking heeft op Interpol, waardoor ze mij het land niet in lieten gaan. De toegang tot Turkije is mij geweigerd zonder geldige reden.’

Burger: ‘Ik kreeg bij aankomst in Sri Lanka te horen dat ik door Interpol was geregistreerd en moest mee naar het kantoor met mijn vrouw. Daar werd ik door 4 à 5 personen ondervraagd. Ik mocht in eerste instantie het land niet in, maar na anderhalf uur uiteindelijk toch. Daarna reisden we door naar Turkije, maar daar werd de toegang geweigerd omdat ik een ‘fout persoon’ zou zijn. Er werd niets gezegd over de reden van weigering of over Interpol. Er werd alleen gezegd dat ze vanuit Nederland een signaal hadden dat ik een fout persoon was. Ik mocht op het vliegveld overnachten.’

Sommige burgers hebben tot een bepaalde datum een inreisverbod in een bepaald land. Eén geïnterviewde burger mag een aantal landen niet meer in en kan daardoor nooit bij zijn schoonfamilie op bezoek. Dat is behoorlijk ingrijpend voor hem. In andere gevallen is het niet altijd duidelijk waarmee mensen nog rekening moeten houden. Ze weten dan niet of ze nog vrij naar alle landen kunnen reizen. Sommige geïnterviewden gaven aan bang te zijn geworden om met hun problemen bij de overheid aan te kloppen. Ze vrezen dat contact met de overheid de situatie voor hen erger kan maken dan die nu is en kiezen ervoor om dan maar niet naar

[10] Zie artikel 8 Handvest grondrechten van de EU: ‘1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens. 2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan. 3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.’

bepaalde landen te reizen. Ze weten immers niet hoe de autoriteiten van die landen zullen reageren en welke risico's ze lopen als ze proberen naar een ander land te gaan. Ook advocaten geven dit aan: burgers zien af van het gebruik van hun rechten, omdat ze een nadelig resultaat vrezen. Dit wordt ook wel een *chilling effect* genoemd.[11]

Advocaat: 'Wij zien een zogenoemd chilling effect bij mensen. Er is geen eenvoudige manier om te weten te komen of er informatie is gedeeld en met wie, en als je daar procedures voor wilt starten, kost dit tijd en geld. Daardoor haken mensen af en doen ze maar niets, of ze reizen niet meer [naar bepaalde landen].'

Uit het bovenstaande blijkt dat het recht op behoud van familie- en gezinsleven in het geding kan komen als burgers door een bepaalde maatregel van de Nederlandse autoriteiten of die van een ander land niet meer in staat zijn om dergelijke banden en contacten te onderhouden.[12] Daarnaast kunnen reisbeperkingen burgers raken in hun recht op bewegingsvrijheid.

Problemen in het binnenland

Hoewel het merendeel van de burgers die wij spraken problemen ondervond (en soms nog steeds ondervindt) bij het reizen en/of doorreizen, merkten ze ook op andere manieren dat ze (vermoedelijk) in de gaten werden gehouden in verband met CTER. Het ging dan bijvoorbeeld om mensen in Nederland die door de politie werden aangesproken (bijvoorbeeld op basis van hun kenteken), vanwege een aandachtsvestiging (een notitie om speciaal op iemand te letten). Een belangenorganisatie vertelde over een burger die meermalen had meegemaakt dat na het scannen van zijn kenteken vele agenten werden opgeroepen en hij werd meegenomen naar het politiebureau. Vervolgens werd hij vrijgelaten en kreeg hij een excuusbrief. Het is hem niet duidelijk waarom dit gebeurde. Eén burger vermoedde dat hij niet werd aangenomen bij de politie vanwege een mogelijke CTER-registratie of informatie op het gebied van CTER.

De ombudsman sprak ook iemand die zich inzet tegen racisme jegens vluchtelingen en op enig moment door een onbekend 06-nummer werd gebeld. Hij wist niet wie hij aan de telefoon had, maar uiteindelijk bleek het de politie te zijn. Die bleek een aantal dingen van hem te weten. De politie gaf aan het vermoeden te hebben dat hij zich met 'serieuze dingen' bezighield. Hij werd uitgenodigd voor een gesprek met de politie, maar wilde daar niet op ingaan. Via een inzageverzoek bij de gemeente kwam hij erachter dat de politie hem online in de gaten hield.

Weer iemand anders vertelde dat hij in de problemen was gekomen doordat de NCTV hem online volgde, waarna hij in de deradicaliseringsaanpak van de gemeente terechtkwam. Hij had daar op dat moment geen weet van. Achteraf bleek dat hij daar ten onrechte in was gekomen. Verder bleek dat de politie deze persoon op enig moment heimelijk volgde, zelfs naar het huis van zijn moeder, om erachter te komen waar hij verbleef.

[11] Het EHRM gebruikt deze term bij de beoordeling van inmenging in grondrechten door de overheid. Bij de beoordeling of een inmenging geoorloofd is, kijkt het EHRM dus ook in hoeverre er sprake is van een chilling effect.

[12] Zie artikel 8 EVRM: '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.' Zie ook artikel 7 Handvest grondrechten van de EU.

Burger: ‘Mijn moeder was toen 78. Ze weigerde de agenten de toegang, maar heeft er wel weken van wakker gelegen.’

Oorzaak problemen onduidelijk
Het kwam hierboven al zijdelings aan de orde: de burgers die de ombudsman heeft gesproken, vertelden bijna allemaal dat ze geen idee hadden waarom ze (extra) werden aangesproken, gecontroleerd, vastgezet of geweigerd. Ze schrokken ontzettend van de gang van zaken en wilden weten waar het probleem zat. Vaak kregen ze dat niet te horen en al helemaal niet direct bij de controle zelf. Een aantal personen gaf aan dat ze bij ondervraging in het buitenland meerdere malen vroegen waarom ze ondervraagd of zelfs vastgezet werden. In een enkel geval kwam daar een minimaal antwoord op. Zo kreeg één burger te horen dat hij genoteerd stond als ‘een fout persoon’ of ‘een gevaarlijk persoon’. Soms werd gezegd dat het land vanuit Nederland informatie had ontvangen, maar niet welke informatie dat was en op basis waarvan dat gebeurde. Of er werd wel gezegd dat er sprake was van een Interpol-registratie, maar niet wat er dan precies in die registratie stond. Meer informatie kregen burgers doorgaans niet. Dat leidde tot grote onzekerheid. Zeker burgers die op reis waren, wisten niet wat hun nog te wachten stond en of ze bijvoorbeeld nog konden doorreizen naar een volgend land. Ook op hun volgende reizen had het invloed. Sommige burgers werden bang om te reizen of besloten zelfs om dat helemaal niet meer te doen.

Burger: ‘Ze zeiden tegen me: u staat te boek als gevaarlijk, u mag vijf jaar het land niet in.’

Burger: ‘Elke keer als ik naar Marokko reis, word ik apart genomen en worden er vragen gesteld. Dit gebeurt nog in Europa. Als ik vraag waarom dit gebeurt, krijg ik geen antwoord.’

Burger: ‘De man die me verhoorde, vroeg: ben je weleens in het Midden-Oosten geweest? Via Google Translate antwoordde ik: nee, never nooit, nergens. Hij schrijft dat op en ik denk: het komt vast goed. Maar hij nam me mee naar een celletje. Na drie dagen zette de politie me in het vliegtuig terug, samen met mijn vrouw. Ik weet nog steeds niet waarvan ze me verdenken. In Nederland zei de marechaussee dat ze niets konden zien.’

Het is volgens de geïnterviewden niet altijd duidelijk aan welke landen informatie is doorgegeven. En verwijdering door de overheid is volgens hen geen garantie dat de informatie dan ook door alle andere landen wordt verwijderd. Bij de geïnterviewde partijen heerst het gevoel dat andere landen het zekere voor het onzekere nemen en informatie niet zomaar verwijderen, wat ertoe kan leiden dat oude informatie iemand blijft achtervolgen.

Inzageverzoeken geven ook geen duidelijkheid
Burgers die problemen hebben ondervonden, willen graag weten wat daarvan de oorzaak is, welke gegevens er over hen zijn vastgelegd en met wie die zijn gedeeld. Ook willen ze weten welke consequenties de gegevens en de gegevensdeling verder nog zullen hebben en wat ze daaraan kunnen doen. Het lastige is dat ze vaak niet weten bij welke instantie ze als eerste moeten aankloppen. Het kan zijn dat er bij meerdere instanties gegevens over hen zijn geregistreerd. Ze weten zelf vaak niet bij welke instanties en weten daarom ook niet waar ze

precies inzageverzoeken kunnen doen. Ook weten ze vaak niet waarín ze precies inzage moeten vragen.

Advocaat: 'Er is wel enige mate van rechterlijke bescherming, maar die is vooral geregeld als je weet welke informatie je moet hebben en bij welke instantie je moet aankloppen. Probleem is vaak dat je niet weet welke stukken er zijn en dat je daar niet achter komt.'

Als burgers een inzageverzoek doen, krijgen ze vaak niet de informatie waar ze naar op zoek zijn (of niet alle informatie), zo geven ze aan. Soms komt er helemaal geen reactie op zo'n verzoek, vertelden burgers en advocaten aan de ombudsman, of een onvolledige reactie. Ze vragen dan bijvoorbeeld om een volledig overzicht van alle over hen geregistreerde informatie die heeft geleid tot de ondervraging, maar krijgen slechts een uitdraai uit het politiesysteem met summiere informatie, waarmee ze niet zijn geholpen. Burgers krijgen ook wel te horen dat de instantie informatie heeft die niet gedeeld kan of mag worden. Of dat er niet verder dan een bepaalde periode kan worden teruggekeken in de systemen, omdat gegevens na een bepaalde tijd worden vernietigd, waardoor niet alles meer valt te achterhalen. Het kan zijn dat de inlichtingendiensten een rol spelen, die (vanwege beperkingen in de Wet op de inlichtingen- en veiligheidsdiensten (Wiv)) nog minder openheid kunnen geven dan andere instanties. Het lukt burgers kortom niet om een compleet beeld te krijgen van wat er is geregistreerd en met wie die informatie is gedeeld. Dat geeft aanhoudende onzekerheid en het idee dat er onterecht zaken worden achtergehouden.

Een geïnterviewde journalist en een advocaat merkten op dat de houding van de overheid over het algemeen onwelwillend en niet meewerkend is. Dat merken ze aan de toonzetting en het contact met de overheid: burgers krijgen vaak een standaardbriefje terug op een inzageverzoek en moeten vervolgens zelf maar uitzoeken wat de volgende stap is.

Journalist: 'Het gaat hier om gevallen die waarschijnlijk jaren geleden hebben gespeeld. Die mensen ondervinden daar nu nog aantoonbaar problemen van. Dan zou je zeggen dat de overheid verplicht is om dit goed uit te zoeken. Die houding van de overheid mis je. Het uitzoeken van informatie gebeurt pas onder juridische druk, of iemand moet zelf met informatie komen.'

Journalist: 'De overheid zegt ook niet: wij zoeken uit wat er aan de hand is of nemen wel contact op met [een ander land]. Als de overheid echt moeite zou doen om dit op te lossen, dan zou zij voor de mensen op de LOP-j-lijst[13] met wie niets aan de hand is, op verzoek en het liefst zelfs actief kunnen aangeven bij andere landen dat zij nu geen reden meer ziet om deze gegevens te bewaren.'

[13] Zie Tweede Kamer, vergaderjaar 2022-2023, 29754, nr. 688, 24 juli 2023. De Landelijk Overzicht Politie – Jihadgang-lijst (LOP-j-lijst) werd gebruikt om binnen de politie zicht te houden op alle personen die destijds betrokken waren bij het uitreizen van personen naar het strijdgebied in onder andere Syrië en Irak.

Advocaat: 'Het behandelen van inzageverzoeken lijkt onbekend bij instanties. Het lijkt alsof er niet voldoende handvatten zijn om een goed besluit op een inzageverzoek te nemen. Men speelt op safe en weigert snel de gevraagde informatie te geven.'

Burger: 'Ik heb een inzageverzoek ingediend bij de Nederlandse politie, waarin ik aangeef kennis te willen nemen van de politiegegevens die over mij zijn verwerkt, wat het doel is van het gebruik van die gegevens en wie de ontvangers daarvan zijn. Daarop kreeg ik een besluit (met een overzicht van mutaties) waarin de onderliggende informatie veelal werd geweigerd met een beroep op de weigeringsgronden in de Wpg. Verder gaf de politie aan dat er voor zover bekend geen politiegegevens verstrekt zijn. Ook staat in het besluit dat het niet is gelukt om alle informatie die bij de Landelijke Eenheid verwerkt is, te achterhalen. De politie gaf aan dat ik nog een apart besluit zou ontvangen als deze informatie binnen was. Dat besluit blijft echter uit.'

Om het verhaal toch compleet te krijgen, doen burgers dan vaak opnieuw een inzageverzoek, bij dezelfde instantie en/of ergens anders. Er ontstaan soms situaties waarin mensen een groot aantal inzageverzoeken doen waar steeds aparte besluiten op worden genomen, maar waarbij ze uiteindelijk niet de zekerheid krijgen dat ze over alle informatie beschikken. Het komt voor dat instanties dit in de hand werken door naar elkaar door te verwijzen, zo geven burgers aan. Ze voelen zich dan van het kastje naar de muur gestuurd. Iemand diende bijvoorbeeld een inzageverzoek in bij de KMar, omdat die over de grensbewaking gaat, maar werd doorverwezen naar de politie. Later bleek toch de KMar het juiste adres. Ook advocaten, een belangenorganisatie en een journalist met wie de ombudsman sprak, bevestigden dat verschillende instanties vaak naar elkaar doorverwijzen.

Belangenorganisatie: 'Uit zowel de ervaringen van demonstranten die wij spreken als onze eigen ervaringen als we informatie opvragen, blijkt dat het heel lastig is om als persoon of als maatschappelijke organisatie informatie op tafel te krijgen over de werkwijze van overheidsinstanties die informatie verzamelen. We zijn geschokt hoe moeilijk het is voor demonstranten om zicht te krijgen op registraties over henzelf en ook hoe moeilijk het is om informatie te krijgen over het beleid en de werkwijze in het algemeen.'[14]

Journalist: 'De waarborgen waarvan de overheid zegt dat ze er zijn, werken niet. Je moet ervan uit kunnen gaan dat als je inzageverzoeken verstuurt, één en ander serieus wordt uitgezocht.'

Als iemand op basis van een inzageverzoek informatie krijgt, wordt daarmee vaak nog niet duidelijk welke gevolgen er kleven aan bepaalde registraties of een gegevensdeling met het buitenland. En wat ervoor nodig is om een signalering in te trekken of registraties ongedaan te maken. In een enkel geval waren instanties uiteindelijk bereid om met iemand in gesprek te gaan om deze en andere vragen op te helderen. Een dergelijk gesprek kan veel duidelijk maken, mits

[14] Demonstranten kunnen ook te maken krijgen met CTER-codes, bijvoorbeeld doordat een CTER-code 05 (dier- of milieu-extremisme) aan een mutatie wordt gekoppeld.

de informatie niet strijdig is met andere informatie die de burger van de instantie heeft gekregen.

Burger: 'Tijdens het gesprek werd het mij duidelijk dat het allemaal is begonnen met een signalering door de politie. Ook kwam ik er in dat gesprek achter dat ik twee jaar lang SIS-[15] gesignaleerd was. (...) Het verbaast mij dat ik pas tijdens het gesprek tekst en uitleg kreeg. Ik denk ook dat ik één van de weinigen ben die zo'n gesprek heeft gekregen. Het is nu erg moeilijk te achterhalen met wie mijn gegevens allemaal zijn gedeeld.'

Advocaat: 'Pas na doorvragen, zelf onderzoek doen, met juridische stappen dreigen, wordt er toch iets gevonden. Burgers moeten slim en vasthoudend zijn, dan is er een kans dat het lukt.'

Uit de verhalen van burgers komt naar voren dat het voor hen een moeizame zoektocht is om duidelijk te krijgen welke informatie is vastgelegd en gedeeld, en of dit terecht en proportioneel was. Daarmee komt hun recht op bescherming van persoonsgegevens in het geding. Dat omvat namelijk ook het recht op informatie over inzageverzoeken en hoe je die moet indienen. Verder weten burgers vaak niet wat hun rechten zijn, waar ze terechtkunnen en hoe ze een eventuele CTER-registratie kunnen aanvechten. Daarmee komt hun rechtsbescherming in het geding. Rechtsbescherming betekent namelijk ook dat burgers moeten kunnen achterhalen wat hun rechten zijn.

In beroep bij de rechter

Wanneer burgers niet of onvoldoende reactie krijgen op hun inzageverzoeken, kiezen ze er soms voor om (al of niet met behulp van een advocaat)[16] bij de bestuursrechter beroep in te stellen tegen de besluiten op hun inzageverzoeken. Dit vraagt een lange adem, tijd, energie en geld. En toch bewandelen sommigen die route in een ultieme poging te achterhalen wat er precies over hen is gedeeld en met wie.

Burger: 'Ik heb met mijn advocaat toch de rechtszaak voortgezet. Ik wil graag weten hoe het zit met alle verwerkingen van mijn persoonsgegevens. Ik wil meer dan alleen antwoord op de vraag of ik SIS-gesignaleerd ben. Hoe zijn mijn gegevens gedeeld met de gemeente en andere instanties? En met welke landen?'

Journalist: 'De rode draad die uit alle dossiers naar voren komt, is dat burgers tot het uiterste moeten gaan om transparantie te krijgen. Iedere keer is er een nieuwe loopgraaf en moet je zelf stappen zetten om verder te komen.'

Een procedure bij de rechter levert ook niet altijd duidelijkheid op, omdat burgers en hun advocaten niet weten welke informatie er is. Het gebeurt ook dat tijdens de juridische procedure blijkt dat er toch meer informatie is.

[15] Het SIS is een Europees informatiesysteem waarin signaleringen kunnen worden opgenomen, bijvoorbeeld om iemand onopvallend te controleren.
[16] In het bestuursrecht is een advocaat niet verplicht.

Advocaat: 'Het blijft ook lastig om met een zaak naar de rechter te gaan, want er is geen dossier. En hoe kom je erachter welke informatie er wel is? De instanties geven geen of weinig informatie. En later blijkt er dan toch soms meer te zijn.'

Sommige burgers kozen ervoor een civiele procedure aan te spannen, omdat ze op een andere manier niet het gewenste resultaat konden bereiken. Dit leverde hun in enkele gevallen een gunstige uitspraak op. Zo is de ombudsman één civiele procedure bekend waarin de rechter het aannemelijk achtte dat iemand schade had geleden door het onrechtmatig handelen van de politie en de Staat door zijn gegevens onzorgvuldig en niet conform de Wet politiegegevens (Wpg) te verwerken. Verder was er een procedure waarin de politie na een aansprakelijkheidsstelling aangaf bereid te zijn om eenmalig via diplomatieke weg contact op te nemen met de autoriteiten van het land waar de burger was geweigerd. De politie zou dan laten weten dat een eventuele eerdere signalering of gegevensverstrekking niet meer actueel was en dat de betrokken burger geen verdachte was in een strafrechtelijk onderzoek.

Wat er beter zou kunnen
De gesprekspartners die in dit hoofdstuk aan het woord komen, hebben benoemd welke verbeteringen zij nodig vinden. Zij noemen vrijwel allemaal dezelfde punten:

Registraties vastleggen en controleerbare toetsing vooraf
De overheid moet volgens de gesprekspartners zorgvuldig vastleggen welke informatie zij verwerkt en welke informatie zij deelt en met wie. Dit geeft mensen duidelijkheid en maakt het makkelijker om een registratie aan te vechten. Daarnaast heeft een journalist de indruk dat een serieuze en individuele toets, voorafgaand aan het delen van informatie met andere landen en naderhand te achterhalen en controleren, ontbreekt.

Journalist: 'De overheid stelt soms dat het om complexe individuele zaken gaat. Maar het gaat in de basis om gegevensdeling waar geen waarborgen voor zijn. Dat is de bottomline van alle gevallen. Je krijgt de indruk dat er geen individuele en onafhankelijke toetsing plaatsvindt; er wordt niet op individueel niveau een afweging gemaakt.'

Laagdrempelige en effectieve procedure voor inzage
De gesprekspartners geven aan dat er meer duidelijkheid nodig is over het waarom van de registratie en het delen van gegevens daarover. Als burgers om inzage vragen, willen ze weten waarom er een registratie op hun naam staat, en welke gegevens er met wie zijn gedeeld. Dit moet op een makkelijker manier te achterhalen zijn, en daarbij moet de overheid zo transparant mogelijk handelen. Als de gevraagde gegevens niet worden verstrekt, moet de overheid goed onderbouwen waarom niet.

Burger: 'Ik wil graag duidelijkheid. Ik vind het niet erg dat ik onderzocht ben. Ik wil zelf ook in een veilig land wonen. Ik heb niks te vrezen. Maar ik wil wel weten welke gegevens over mij gedeeld zijn binnen en buiten Nederland en met wie.'

Advocaat: 'Instanties moeten beter omgaan met inzageverzoeken en beter hun best doen bij de afhandeling van die verzoeken. Het is aan de overheid om toegang te geven tot de informatie, terwijl er nu continu sprake is van touwtrekken. Niemand van de politie zegt: kom maar, ik pak je bij de hand, je krijgt een maximaal en eerlijk antwoord.'

Over een handreiking aan burgers met informatie over de inzageprocedure zijn de meningen verdeeld. Eén burger zei een handreiking zinvol te vinden. Maar volgens een advocaat gaat het er niet om dat mensen geïnformeerd worden over hóe zij inzage moeten vragen. Het gaat erom dat als iemand een instantie benadert, dat die daadwerkelijk iets doet met een inzageverzoek.

Advocaat: 'Het gaat fout omdat instanties een beslissing nemen waar je feitelijk niets mee kunt. Je weet niet of het besluit goed is of niet. En krijg je een besluit, dan geloof je het niet meer, omdat er te veel fouten zijn gemaakt. Het oplossen hiervan is een intern probleem, het gaat er niet om dat burgers iets anders moeten doen. Dit los je niet op met een handreiking aan betrokkenen.'

Er is bij burgers behoefte aan één centraal aanspreekpunt waar ze met vragen terechtkunnen. Zo'n aanspreekpunt zou een efficiënte en laagdrempelige ingang moeten zijn om na te gaan welke informatie er is vastgelegd en gedeeld. Zo krijgen ze een volledig overzicht en duidelijkheid over hun situatie. Ook kunnen mensen van dat centrale punt informatie krijgen over de mogelijke gevolgen van een CTER-registratie en hoe ze daar iets tegen kunnen ondernemen.

Erkenning en verantwoordelijkheid nemen
Burgers willen ook dat de overheid actieve hulp biedt om registraties te verwijderen en de gevolgen ervan ongedaan te maken. Ook als er informatie is gedeeld met andere landen. Het moet duidelijk zijn wat iemand kan doen als er informatie is gedeeld en hoe de schade daarvan kan worden beperkt.

Advocaat: 'De overheid moet via diplomatieke kanalen proberen om de informatie bij andere landen verwijderd te krijgen. De Nederlandse overheid weet met wie die informatie gedeeld is, zoals Schengenlanden, en via welke kanalen, zoals Interpol. Dit zijn vaak dezelfde landen en soms ook het land waarmee iemand banden heeft op grond van herkomst.'

Burgers willen verder dat de overheid het probleem erkent en verantwoordelijkheid neemt.

Burger: 'Erkenning is stap één. Nationale veiligheid is mooi, maar niet ten koste van honderden personen. Dat is buitenproportioneel.'

De partijen waarmee de ombudsman heeft gesproken, willen graag meer aandacht voor (betere) rechtsbescherming van burgers. Ze geven aan dat de overheid op dit moment vooral beslissingen neemt op basis van het systeem en met name oog heeft voor de nationale veiligheid en niet voor de mensen die hier het slachtoffer van worden.

Wetenschapper: ‘Ik heb met demonstranten gesproken die door de politie zijn gecontroleerd terwijl daar volstrekt geen aanleiding voor was. De politie is heel actief in het verzamelen van gegevens en het is niet duidelijk wat daar verder mee gebeurt. Op deze manier staat ook het demonstratierecht onder druk.’

Wetenschapper: ‘Problematisch is dat de overheid een systeem bedenkt en het vervolgens niet in de hand heeft. De overheid heeft geen grip op het delen van gegevens en de gevolgen die dat kan hebben. Als je iets doet [als overheid] moet je het ook ongedaan kunnen maken. Dat lijkt nu niet het geval.’

Wetenschapper: ‘Het is cynisch dat sommige landen deze mensen niet van hun lijsten willen halen. Zoals de Verenigde Staten (VS). In die zin is het dus heel moeilijk om de praktische problemen van deze mensen op te lossen. Maar dat maakt juist dat je vooraf heel goed moet nadenken over wie er op zo’n lijst komt. Het delen van gegevens moet al op lokaal niveau uiterst zorgvuldig gebeuren. Aangemerkt staan als terrorist is een zeer zwaar label waar je de rest van je leven niet meer vanaf komt met de huidige veiligheidssystemen.’

3 Perspectief van de overheid

3.1 Inleiding

Het perspectief van de overheid is gebaseerd op gesprekken met medewerkers van de politie, de KMar, het OM, het ministerie van JenV, de NCTV en de AP en op Kamerstukken (antwoorden op Kamervragen, Kamerbrieven en verslagen van debatten).

3.2 Standpunten overheidsinstanties

In deze paragraaf geven we weer welke dilemma's onze gesprekspartners zien rond de problemen die de aanleiding vormden voor dit onderzoek.

Veranderende context

In gesprekken met medewerkers van het ministerie van JenV, de NCTV, de politie en de KMar komt naar voren dat het belangrijk is om oog te hebben voor de context waarin de overheidsinstanties handelen en hebben gehandeld als het gaat om CTER.[17] Het ministerie legt uit dat het beleid in 2012 en de jaren daarna vooral gericht was op het voorkomen van uitreizen naar jihadistisch strijdgebied, waarna burgers – na een mogelijke terugkeer – een gevaar voor de nationale veiligheid zouden vormen. Ook vonden er in die periode grote terroristische aanslagen plaats in Europa. Het wettelijke kader van destijds is dus vastgesteld in een context waarin het veiligheidsbelang vooropstond en zeer urgent werd. Dat is ook terug te lezen in het Dreigingsbeeld Terrorisme van maart 2013,[18] naar aanleiding waarvan het dreigingsniveau is verhoogd naar 'substantieel'. Ook de KMar onderstreept dat de context waarin CTER-verwerkingen plaatsvinden van belang is. Naar aanleiding van de aanslagen in Parijs (2015) en Brussel (2016) is de KMar gestart met het informatieknooppunt CTER.

In de jaren 2012 tot 2018 hield de politie een overzicht bij van (potentiële) uitreizigers: de Landelijk Overzicht Politie – Jihadgang-lijst (LOP-j-lijst). Daarop stonden de burgers die daadwerkelijk waren vertrokken, maar ook burgers van wie werd aangenomen dat ze de intentie hadden om uit te reizen en mensen die behulpzaam waren bij het uitreizen. Er stonden enkele honderden burgers op deze lijst. De overheidsinstanties geven aan dat het delen van deze lijst met andere landen (zoals de VS en Turkije) gebeurde in de context van die tijd en onder druk van het grote aantal personen dat bereid leek te zijn uit te reizen naar het strijdgebied, de zorgen vanuit de directe omgeving van uitreizigers en de dreiging die van uitreizigers kon uitgaan. Volgens de gesprekspartners van het ministerie moest op dat moment adequaat en snel worden gehandeld. Het delen gebeurde toen binnen (inter)nationale wettelijke kaders, aldus de gesprekspartners, maar ook toen was het integraal delen van een lijst ongebruikelijk. Ten opzichte van Turkije en de VS gold het vertrouwensbeginsel. Dat betekent dat Nederland ervan uitging dat de personen op deze lijst een voldoende beschermingsniveau hadden.

Ook de politie geeft aan dat er in de periode van de uitreizigersgolf sprake was van grote politieke druk om veel informatie vast te leggen en mensen te signaleren; de politie mocht geen signaal missen. Dat was geen keuze van de politie zelf, zo stelt zij. De politie werd geacht alle mogelijkheden in de wet- en regelgeving te benutten en alles in het werk te stellen om te voorkomen dat (potentiële) uitreizigers op reis gingen, dat mensen naar het strijdgebied

[17] In dat kader verwijzen instanties naar de Nationale Contraterrorisme Strategie 2022-2026 en het daarin opgenomen uitgangspunt: 'Terrorisme vraagt vanwege de ernst het uiterste van de in te zetten middelen. Idealiter juist preventief; tijdig om geweld te voorkomen. Inperking van grondrechtelijke vrijheden is soms onvermijdelijk, maar wordt zeer kritisch afgewogen. Maatregelen moeten dreigingsgericht zijn, proportioneel, met een stevige wettelijke grondslag. Hierbij handelen de verschillende partners in de CT-aanpak conform de voor hen geldende wettelijke kaders.'
[18] Zie Dreigingsbeeld Terrorisme van 13 maart 2013.

vertrokken en dat er (terroristische) aanslagen werden gepleegd.[19] Tegenwoordig heeft Nederland met deels dezelfde, maar ook met nieuwe dreigingen te maken.

Het ministerie van JenV merkt op dat het aantal nieuwe uitreizigers in de afgelopen jaren sterk is afgenomen en dat tegelijkertijd wetgeving op het gebied van privacy in werking trad, bijvoorbeeld de Algemene verordening gegevensbescherming (AVG). Dit heeft invloed gehad op de verhouding tussen privacy en gegevensdeling ten behoeve van opsporing en inlichting. Hoewel er nu minder uitreizigers zijn, is de terrorismedreiging toegenomen. Daarnaast zijn er andere vormen van extremisme en radicalisering opgekomen (bijvoorbeeld anti-institutioneel extremisme). Volgens de gesprekspartners is het de taak van de officier van justitie om steeds af te wegen of bepaalde maatregelen of inbreuken in verhouding staan tot het doel. Overigens kan het gebeuren dat er afwegingen worden gemaakt die achteraf niet juist blijken. Maar dat betekent niet per se dat er – met de kennis die destijds beschikbaar was – een onjuiste beslissing is genomen, aldus de gesprekpartners. Ten opzichte van vroeger is het proces rond CTER-registraties nu wel meer geformaliseerd en is het duidelijker wie wat doet, zo wordt aangegeven.

Ongenuanceerd beeld in de buitenwereld

De politie hecht er waarde aan meer duidelijkheid te geven over de oorsprong van de problemen rond signaleringen. In de buitenwereld bestaat het beeld dat de oorsprong hiervan altijd bij de politie ligt, terwijl maar een deel van de signaleringen van de politie afkomstig is en vaak ook niet duidelijk is waardoor iemand problemen ondervindt. Bovendien kunnen reisproblemen voortkomen uit informatie die niet van de Nederlandse autoriteiten komt. De politie onderkent dat de systematiek rond CTER-gerelateerde signaleringen complex is. Daar komt bij dat de politie naar de buitenwereld niet altijd (volledige) openheid van zaken kan geven omwille van de nationale veiligheid, de privacy van personen, of opsporingsbelangen. Het ministerie van JenV benoemt dit ook. Dit leidt er soms toe dat er zaken in de media komen die niet altijd het volledige of juiste beeld geven. Ook het OM geeft aan dat het CTER-proces en -systeem veel genuanceerder liggen dan de media laten zien. De politie onderschrijft dit. Eén van de gesprekspartners vertelt dat de buitenwereld weinig zicht heeft op het werkproces: ‘De ene keer doen OM en politie te veel, de andere keer weer te weinig. Terwijl het vaak veel genuanceerder ligt dan in de media wordt geschetst.’

Transparantie versus veiligheid

In meerdere gesprekken komt naar voren dat overheidsinstanties zich – in de communicatie met de buitenwereld (samenleving en politiek) – in een spanningsveld bevinden waarin ze vaak het belang van transparantie en het belang van veiligheid, zowel nationaal als individueel, tegen elkaar moeten afwegen. Over de verwachtingen van burgers zegt de politie dat die graag transparantie willen over de gegevens die de politie heeft verwerkt. De politie begrijpt dit en streeft dit na, zo geeft zij aan, maar stelt tegelijkertijd dat openheid maar tot op zekere hoogte mogelijk is in verband met de nationale veiligheid, de privacy van (andere) personen of opsporingsbelangen (zie artikel 27 Wpg). ‘Niet alles kan openbaar worden gemaakt, vanwege het doel om onopvallende controles van reisbewegingen uit te voeren en zo het reizen van (potentiële) uitreizigers, het reizen naar strijdgebied en een (potentiële) aanslag te voorkomen. Dat maakt het heel lastig.’ Ook als het gaat over de werkwijze van de politie geeft zij aan dat bepaalde informatie niet gedeeld kan worden. Zo wil de politie niet openbaar maken welke indicatoren zij gebruikt om een risicotaxatie uit te voeren, omdat burgers met kwade bedoelingen daaruit kunnen afleiden hoe ze onder de radar kunnen blijven.

[19] Dat werd bijvoorbeeld gedaan via signaleringen ter onopvallende controle van personen die in beeld waren, maar, om uitreizen te voorkomen, ook op basis van waarnemingen bij de grenspassage of in de aanloop daarnaartoe.

Weinig mogelijkheden na informatiedeling met andere landen
Zowel in het gesprek met het ministerie als in Kamerstukken wordt aangegeven dat de afweging van andere landen om mensen tijdens het reizen tegen te houden of te ondervragen moeilijk is te achterhalen. Zij kunnen andere of aanvullende informatie tot hun beschikking hebben. Nederland heeft niet in de hand wat andere landen met de informatie doen. Nederland mag namelijk niet in de rechtsorde van andere landen treden. Daarom is het ook lastig om andere landen te vragen waarom iemand bij hen op een lijst staat of gesignaleerd is, zo vertelt een gesprekpartner vanuit het ministerie. Ook de toenmalige minister van JenV onderstreepte in een Kamerdebat dat het handelingsperspectief van de Nederlandse regering beperkt is als het gaat om signaleringen door andere landen en dat niet valt uit te sluiten dat mensen ten onrechte (nog) gesignaleerd staan.

Het ministerie geeft aan te vermoeden dat een deel van de burgers die nu problemen ondervinden en zich melden, in het verleden in verband zijn gebracht met burgers met een CTER-registratie of in de periferie van een onderzoek in beeld waren. Zij zijn volgens het ministerie binnen de destijds geldende wettelijke kaders gesignaleerd. Het OM geeft aan dat burgers alleen werden gesignaleerd als er aanwijzingen waren voor terroristische misdrijven, zoals uitreizen naar het strijdgebied, deelname aan de gewapende strijd in Syrië en Irak en aansluiting bij terroristische organisaties aldaar. Nederland mocht op basis van juridische kaders informatie delen met landen waarvoor het vertrouwensbeginsel gold, aldus het ministerie. Het kan zijn dat deze mensen nu geen *person of interest* meer zijn en dat de signalering is verwijderd, maar dat ze nog wel problemen ondervinden. Dat kan komen doordat andere landen een eigen afweging maken over wat zij met de informatie doen of een eigen informatiepositie hebben waar zij naar handelen. Het blijft volgens het ministerie heel lastig om bij andere landen te achterhalen wat de reden voor hun handelen is. Bovendien is het ingewikkeld om bij landen aan te geven dat iemand voor Nederland geen *person of interest* meer is. Ieder land maakt daarin uiteindelijk zijn eigen afweging. De autoriteiten in Nederland hebben niet altijd zicht op de redenen van andere landen om iemand te weigeren en op basis van welke informatie dat gebeurt. Voor deze problematiek verwachten de gesprekspartners geen kortetermijnoplossing. Daardoor is het in bepaalde gevallen lastig na te gaan wat er precies aan de hand is.

Ook de politie en de KMar herkennen dit. Volgens de gesprekspartners van de politie komt het voor dat andere landen sommige mensen die gesignaleerd staan een toegangsverbod geven. Dat kan omdat elk land een soevereine verantwoordelijkheid heeft voor de toelating tot het eigen grondgebied. Landen kunnen dit besluit nemen op basis van hun informatiepositie en hun eigen methoden. Daarbij merken ook deze gesprekspartners op dat de Nederlandse autoriteiten meestal geen zicht hebben op eventuele andere informatie over de betrokkenen waar deze landen een dergelijk besluit op baseren. De KMar geeft aan dat het kan voorkomen dat een signalering bij andere diensten of internationaal nog altijd van kracht is. Andere landen hanteren andere wet- en regelgeving en hebben andere normen en waarden.

Veel onduidelijk voor burgers
Als het gaat om CTER-registraties, onderstrepen de gesprekspartners vanuit de overheidsinstanties het belang om ‘het thans onvolledige narratief over dit onderwerp in de buitenwereld beter voor het voetlicht te krijgen.’ Tegelijkertijd merken ze op dat de complexiteit van de systematiek het niet makkelijk maakt om volledige duidelijkheid te bieden aan burgers. Zo worden met betrekking tot CTER-registraties verschillende termen gebruikt, zoals *vinkje* en *registratie*. Het is voor de buitenwereld niet altijd duidelijk wat daar precies mee wordt bedoeld. ‘Dat is ook logisch, het is immers specialistische materie.’ Daardoor bestaat de kans dat door verschillende interpretaties van termen dingen een eigen leven gaan leiden, aldus de politie.

Het OM geeft aan bekend te zijn met de verhalen uit de media van burgers die vertellen dat het lastig is om bij verschillende instanties en loketten informatie te moeten vragen. ‘Je moet net het juiste adres hebben.’ Het OM onderschrijft dat mensen goed moeten weten waar ze terechtkunnen. Onder coördinatie van het ministerie van JenV wordt gewerkt aan een handreiking voor burgers die hinder ondervinden, bijvoorbeeld bij het reizen, en die willen achterhalen wat de oorzaak is van hun problemen. Daarin zal worden uitgelegd hoe burgers en/of hun vertegenwoordigers inzage kunnen krijgen in de persoonsgegevens die zijn geregistreerd en hoe ze daartegen (indien gewenst) bezwaar kunnen maken. Het is volgens de gesprekpartners belangrijk dat in de beloofde handreiking ook adressen en telefoonnummers komen te staan, zodat het voor burgers echt duidelijk is bij wie ze met welke vragen terechtkunnen.

De AP merkt op dat er – in het kader van rechtsbescherming – voor CTER-registraties duidelijke wettelijke normen zijn met goed uitgewerkte mogelijkheden voor burgers. Die lijken echter onvoldoende bekend te zijn bij burgers. De AP geeft bovendien mee dat de politie en justitiële instanties burgers veel beter en actiever zouden kunnen informeren over hun rechten. Maar de toezichthouder trekt zich dat zelf ook aan en wil in de nabije toekomst actiever voorlichting gaan geven over zijn (wettelijke) taak en bevoegdheden.

4 CTER-proces

4.1 Inleiding

In dit hoofdstuk beschrijft de Nationale ombudsman op hoofdlijnen het huidige CTER-proces en welke maatregelen hieruit kunnen volgen. De gesprekken die de ombudsman met overheidsinstanties heeft gevoerd, vormen de basis voor dit hoofdstuk.

4.2 Historische context

Allereerst plaatsen we de CTER-registraties beknopt in een historische context. In 2010 en 2011 zijn binnen de politie intelcellen[20] opgericht die zich specifiek richtten op (mogelijke) uitreisbewegingen van Nederlanders naar jihadistische strijdgebieden. Door middel van vroegsignalering probeerde de politie (mogelijk) geradicaliseerden en (potentiële) uitreizigers eerder in beeld te krijgen, zodat – waar nodig – maatregelen konden worden getroffen. Deze intelcellen moesten de signalen die de politie in het kader van vroegsignalering verzamelde, in eerste instantie beoordelen en eventuele individuele maatregelen voorstellen aan het bevoegd gezag: in de regel het OM.

In 2013 werd de wereld geconfronteerd met een nieuw jihadistisch strijdgebied in Syrië en Irak, waar ISIS in 2014 een kalifaat uitriep. Vanuit Nederland nam het aantal personen dat vertrok om daar deel te nemen aan de gewapende strijd snel toe.[21] Nederlandse instanties hadden hier weinig zicht op, terwijl de zorgen bij zowel families als Nederlandse instanties over deze ontwikkelingen groot waren. Vanwege het ontbreken van protocollen en werkafspraken op dit toen nog nieuwe terrein was de informatie die de opsporingsdiensten voorhanden hadden tot dat moment nog erg versnipperd. Om een beeld te krijgen van de burgers die mogelijk zouden uitreizen of dit faciliteerden, is de politie informatie gaan bijhouden in de zogenoemde *LOP-j-lijst*. Op deze lijst stonden behalve degenen die daadwerkelijk vertrokken ook mensen waarvan werd aangenomen dat ze de intentie hadden om uit te reizen (vanwege hun uitspraken of door een eerdere mislukte poging) en mensen die anderen behulpzaam waren bij het uitreizen (de zogeheten facilitators en ronselaars). Personen die zich aansloten bij niet-jihadistische strijdgroepen kwamen niet op die lijst.[22] Uiterlijke kenmerken zoals een (lange) baard waren geen reden voor plaatsing op de LOP-j-lijst, omdat dit geen bewijs was dat iemand wilde uitreizen of het uitreizen bijvoorbeeld faciliteerde. Ook alleen contact hebben met iemand op de LOP-j-lijst was onvoldoende om zelf op de lijst te worden geplaatst, aldus het OM.

De LOP-j-lijst werd in die periode een aantal keren in zijn geheel gedeeld met de autoriteiten van een aantal Schengenlanden, waaronder Duitsland en België, en derde landen als Turkije en de VS.[23] De politie geeft aan dat Turkije de informatie op de LOP-j-lijst destijds heeft overgenomen in zijn nationale systeem. Tot slot is de lijst gedeeld met Europol. Nederland ontving zelf van andere landen een vergelijkbare lijst. Het doel van de informatiedeling was om reisbewegingen van (potentiële) uitreizigers op een onopvallende manier te controleren en hen ervan te weerhouden naar strijdgebieden te reizen. De LOP-j-lijst was bedoeld om de eigen informatiepositie te versterken, informatie te delen en potentiële uitreizigers tegen te houden bij

[20] De kerntaak van een intelcel is het maken van 'veiligheidsinformatieproducten' door informatie te verzamelen, veredelen en analyseren met als doel overzicht, inzicht en vooruitzicht te bieden voor de sturingsprocessen. Dat bevorderde de samenwerking tussen medewerkers, beslissers en (convenant)partners bij het voorkomen en/of oplossen van veiligheidsproblemen.
[21] In het Dreigingsbeeld Terrorisme van 13 maart 2013 staat beschreven dat het aantal jihadreizigers eind 2012 plotseling zeer snel steeg en dat het vanuit Nederland om tientallen personen ging. Het dreigingsniveau werd verhoogd naar 'substantieel'.
[22] Zie Tweede Halfjaarbericht politie 2023 van 7 december 2023, Tweede Kamer, vergaderjaar 2023-2024, 29628, nr. 1193, bijlage 2, p. 39-40.
[23] Met de term 'derde landen' wordt bedoeld de landen buiten de EU, met uitzondering van de landen die wel onderdeel zijn van de Europese Economische Ruimte. Dit zijn Noorwegen, Liechtenstein en IJsland.

de grens van het strijdgebied. Omwille van diezelfde doelen zijn de personen op de lijst – in overleg met het OM – in 2014 en 2016 internationaal gesignaleerd, zowel via het SIS als via een Interpol *diffusion* (een Interpol-signalering die alleen met bepaalde andere landen wordt gedeeld).[24] Omdat het signaleringen voor onopvallende controle betrof, achtte het OM dit een proportionele maatregel.[25] Bij een onopvallende controle mag de ontvangende partij geen maatregelen nemen; de informatie moet worden verzameld op een onopvallende manier en zonder dat de betrokken persoon daar weet van heeft. Desondanks kan een ontvangend land altijd autonome afwegingen maken, bijvoorbeeld omdat het een eigen informatiepositie heeft waardoor er andere of meer informatie bekend is.

De LOP-j-lijst wordt sinds 2018 niet meer gebruikt.[26] Sindsdien wordt er niet meer afgeweken van de standaardwerkwijze en weegt het OM in alle gevallen per casus af of informatie-uitwisseling met het buitenland is toegestaan en of een internationale signalering noodzakelijk en proportioneel is.[27] Toch is de context waarin de LOP-j-lijst werd gebruikt belangrijk, omdat die inzicht geeft in hoe er in het verleden is gehandeld. Op de LOP-j-lijst hebben ongeveer 400 personen gestaan gedurende de gehele bestaansperiode van de lijst.

Na de terroristische aanslagen in Parijs in 2015 en in Brussel in 2016 ontstond de politieke wens om meer proactief, alert en assertief te handelen op het gebied van terrorismebestrijding.[28] En om, in afstemming met het bevoegd gezag, de grenzen van de wet op te zoeken. Eén van de verdachten van die aanslagen was via Nederland gereisd zonder dat de Nederlandse opsporingsdiensten en grensbewaking daarvan op de hoogte waren. Daarom werd besloten dat er een landelijke aanpak moest komen: het Nationaal Terrorisme Beeld (NTB). Dat is in 2018 ingevoerd. Het hield in dat er niet alleen naar het 'klassieke jihadisme' en de uitreizigers werd gekeken, maar ook naar radicalisering en extremisme in bredere zin. De huidige aanpak is toen ontstaan.

4.3 Proces op hoofdlijnen

In deze paragraaf beschrijven we het proces vanaf een eerste CTER-registratie (het toekennen van een CTER-projectcode aan een gebeurtenis) tot aan plaatsing op de afstemmingslijst en eventuele maatregelen die tegen burgers kunnen worden genomen.[29] Het gaat daarbij om de huidige werkwijze van de betrokken instanties (politie, KMar, OM). Niet alle stappen hoeven altijd te worden doorlopen: bij elke stap volgt een afweging of het nodig is om naar de volgende stap te gaan.

We beschrijven niet de situatie waarin een signaal uitmondt in een strafrechtelijk onderzoek en vervolging. In dat geval geldt een ander traject. Bij de klachten die de aanleiding vormden voor dit onderzoek, was geen sprake van daadwerkelijke strafrechtelijke vervolging en ging het juist om het (voor burgers onzichtbare) proces van informatieverzameling en -deling van burgers die veelal geen verdachte zijn van een strafbaar feit.

[24] De landen die hierbij worden genoemd zijn: Montenegro, Servië, Turkije, Georgië, Kosovo, Cyprus, Gibraltar, Monaco, Andorra, Bosnië en Herzegovina, Albanië, San Marino, Groot-Brittannië, Ierland, Noord-Macedonië en Israël.
[25] Zie paragraaf 4.4 voor meer uitleg over signaleringen.
[26] Bij de start van het NTB-proces is de lijst gecheckt en is per individuele casus overwogen en afgestemd met het OM of deze persoon op de afstemmingslijst geplaatst moest worden.
[27] Het OM geeft aan dat ook het onderscheid tussen Schengenlanden en derde landen van belang is en of er internationale verdragen zijn afgesloten. Zo heeft de Raad van Europa met landen rechtshulpverdragen afgesloten. Nederland en Turkije zijn beide lid van het Europees Verdrag aangaande de wederzijdse rechtshulp in strafzaken. De Raad van Europa heeft daarmee het vertrouwen in Turkije uitgesproken voor de internationale uitwisseling van informatie in strafzaken.
[28] Dit blijkt onder andere uit de gestelde vragen en moties in de debatten over de aanslagen in Parijs (19 november 2015) en Brussel (29 maart 2016 en 7 april 2016).
[29] Het gaat grofweg om de volgende aantallen: stap 1: 3000 CTER-registraties, stap 2: 1000 CTER-waardige registraties, stap 3: tienduizenden burgers in het themaregister en stap 4: enkele honderden burgers op de afstemmingslijst.

De KMar heeft een zelfstandige rol in de CTER-aanpak en heeft aansluiting gezocht bij de manier waarop de politie het proces heeft georganiseerd. De KMar kan potentieel CTER-waardige signalen registreren en aanleveren bij de betreffende intelcel van de politie. Daar waar de processen van de politie en de KMar van elkaar verschillen, hebben we dat beschreven.

Van de toekenning van een CTER-projectcode tot het nemen van maatregelen

Stap 1	Toekenning CTER-projectcode ↓	• Handhavingsinformatie • Vroegsignalering
Stap 2	Duiding van CTER-projectcode door CTER-intelcel ↓	• Beoordeling CTER-waardigheid • Duiding op soort CTER-projectcode
Stap 3	Opname in het themaregister ↓	• De CTER-registratie wordt verder aangevuld met informatie en de betrokken perso(o)n(en) wordt/worden nader geduid. Het gaat niet om getuigen.
Stap 4	Plaatsing op afstemmingslijst ↓	• In overleg met het bevoegd gezag (OM) • Passieve of actieve monitoring
Stap 5	Maatregelen	• In overleg met het bevoegd gezag (OM)

Stap 1: toekenning van een CTER-projectcode
Als politieagenten signalen van mogelijk terrorisme, extremisme of radicalisering zien of vernemen, dan kunnen zij een registratie aanmaken in de Basisvoorziening Handhaving (BVH). Ze geven daarbij een feitelijke weergave van de mogelijke CTER-gebeurtenis en kennen in dat geval ook een CTER-projectcode toe aan de registratie van de gebeurtenis (de code wordt dus niet aan een persoon gekoppeld). Zo'n registratie is doorgaans afkomstig van een politieambtenaar die direct in contact staat met burgers, zoals een wijkagent. Tijdens de politieopleiding krijgen agenten een specifieke training om dit soort signalen te herkennen, maar ook daarna blijft dit een continu trainingsproces.

In het kader van de CTER-aanpak luidt de opdracht aan agenten: registreer zo uitgebreid mogelijk in de BVH. Hierbij gaat het om gedragingen of gebeurtenissen die in het kader van de politietaak opvallend ogen. Als er bijvoorbeeld in of bij een woning een vlag hangt met bepaalde (mogelijk extremistische of terroristische) symbolen, zou dat kunnen wijzen in de richting van extremisme. Hoewel dat niet het geval hoeft te zijn, kan de politieambtenaar het waarnemen van de vlag als gebeurtenis opnemen in de BVH. De verdere beoordeling van de gebeurtenis behoort niet tot de taken van de betreffende politieambtenaar.

De politie hanteert sinds 2023 de volgende definities van terrorisme, extremisme en radicalisering:

- Terrorisme: 'Het uit ideologische motieven (voorbereiden van het) plegen van op mensenlevens gericht geweld, of het veroorzaken van maatschappij ontwrichtende schade, met als doel (een deel van) de bevolking ernstige vrees aan te jagen, maatschappelijke veranderingen te bewerkstelligen en/of de politieke besluitvorming te beïnvloeden.'[30]
- Extremisme: 'Het vanuit een bepaalde overtuiging willen afdwingen van maatschappelijke veranderingen of politieke besluitvorming en daartoe activiteiten uitvoeren waarmee in meer dan geringe mate de wet wordt overtreden.'
- Radicalisering: 'Groeiende bereidheid tot het nastreven en/of ondersteunen van diep ingrijpende veranderingen in de samenleving die op gespannen voet staan met de democratische rechtsorde en/of waarbij ondemocratische middelen worden ingezet.' [31]

Ook een medewerker van de KMar kan een CTER-projectcode toekennen aan een gebeurtenis. Dat gebeurt als het vermoeden bestaat dat een gebeurtenis CTER-gerelateerd zou kunnen zijn. Deze registratie komt in het Bedrijfsprocessensysteem (BPS) van de KMar. Net als bij de politie hebben de operationele medewerkers van de KMar een CTER-opleiding gevolgd.

Stap 2: van toekenning van een CTER-projectcode naar duiding op persoonsniveau
Als een ambtenaar van de politie of de KMar een CTER-projectcode aan de registratie van een gebeurtenis toevoegt, dan wordt deze gebeurtenis automatisch onder de aandacht gebracht van een CTER-intelcel van de politie of de KMar. Een CTER-intelcel verzamelt, verwerkt, duidt en verstrekt veiligheidsinformatie over activiteiten, personen en groepen die in verband kunnen worden gebracht met het thema CTER. Daarmee beoogt de CTER-intelcel om signalen van radicalisering in een vroegtijdig stadium op te vangen en, waar mogelijk in coördinatie met andere afdelingen en instanties, te interveniëren.

Na ontvangst van een registratie waaraan een CTER-projectcode is gekoppeld, maakt een CTER-intelcel de afweging of de gebeurtenis (niet de persoon) daadwerkelijk CTER-waardig is of niet. Bij die beoordeling zal de intelcel meer informatiebronnen raadplegen dan alleen de verkregen informatie van de politieambtenaar.

De politie gebruikt de volgende definitie voor het bepalen van de CTER-waardigheid:

'Mogelijk signaal dat vanuit een bepaalde overtuiging maatschappelijke veranderingen of politieke besluitvorming wordt afgedwongen en daartoe activiteiten worden uitgevoerd waarmee in meer dan geringe mate de wet wordt overtreden.'[32]

De CTER-intelcel maakt eerst een grove selectie van registraties die direct als niet-CTER-waardig kunnen worden beschouwd en registraties die nog nadere aandacht nodig hebben. Vervolgens kijkt de intelcel naar het totaalbeeld van de gegevens en alle eerdere informatie over de gebeurtenis die binnen de politie beschikbaar is. De intelcel betrekt daarbij ook openbare bronnen, zoals sociale media.

[30] Dit is de definitie die de NCTV hanteert, evenals de CT-partners, zoals de politie en de KMAR.
[31] De politie wijkt met deze definities van extremisme en radicalisering af van de definitie die de NCTV gebruikt.
[32] Dit is de definitie van 'extremisme' die de politie hanteert.

Na deze afweging kent de intelcel één van de volgende codes toe aan de CTER-registratie:

CTER01	CTER ALGEMEEN (wordt ook gebruikt voor anti-institutioneel extremisme)
CTER02	JIHADISME
CTER03	NIET-JIHADISTISCH RELIGIEUS EXTREMISME
CTER04	LINKS-EXTREMISME
CTER05	DIER- OF MILIEU-EXTREMISME
CTER06	RECHTS-EXTREMISME
CTER07	SEPARATISME
CTER08	NIET CTER-WAARDIG

Bij de KMar duidt de intelcel van de KMar alle door KMar-medewerkers geregistreerde signalen. Als een gebeurtenis volgens de KMar CTER-waardig is, wordt die ingevoerd in het systeem van de politie, waarna de politie er verder naar kijkt.

De registratie in de BVH (politie) en het BPS (KMar) met CTER01-CTER08 wordt vijf jaar bewaard vanaf het moment van registratie, samen met de oorspronkelijke registratie van de politieambtenaar of KMar-medewerker, zoals bepaald in de Wpg (artikel 8 lid 6 Wpg).[33] Als de bewaartermijn verloopt, wordt de registratie verwijderd. Dat houdt in dat de informatie nog wel vijf jaar 'achter een schot' wordt bewaard, voor bijvoorbeeld het afhandelen van klachten en de verantwoording van verrichtingen (zie artikel 14 Wpg). De informatie is dus nog wel aanwezig, maar niemand kan er meer bij, tenzij er een zwaarwegende en goed onderbouwde reden voor is. Deze informatie wordt ook geraadpleegd bij een eventueel inzageverzoek.

Niet CTER-waardig: code 08
Wanneer een gebeurtenis volgens de intelcel niet CTER-waardig is, koppelt de intelcel dit terug door in de BVH de code CTER08 op te nemen. Dit gebeurt met ongeveer 60 procent van de oorspronkelijke CTER-registraties. De 08-code blijft conform de Wpg vijf jaar zichtbaar in de BVH.[34] Daarna wordt niet alleen de code, maar de gehele registratie verwijderd. De politie verwijdert de CTER-code niet gedurende die vijf jaar, omdat zij het relevant vindt deze informatie te bewaren. Wanneer een eerdere gebeurtenis kan meewegen als context, kan een volgende gebeurtenis met dezelfde betrokkene(n) namelijk wél CTER-waardig worden bevonden. Daarnaast is het volgens de politie ook voor burgers zelf belangrijk dat een gebeurtenis die niet-CTER-waardig was geregistreerd blijft. De afweging van de intelcel wordt bewaard bij de oorspronkelijke registratie. Daardoor is gedurende de bewaartermijn van vijf jaar ook de afweging van de CTER-intelcel over de niet-CTER-waardigheid te zien.

Stap 3: opname in het themaregister CTER
Als de intelcel na de beoordeling/analyse van mening is dat een gebeurtenis CTER-waardig is, neemt deze intelcel de betrokken persoon of personen op in het themaregister CTER. Een themaregister wordt gebruikt om inzicht te krijgen in de mogelijke betrokkenheid van personen

[33] De politie licht toe dat er in de BVH meer staat dan alleen artikel 8 Wpg-informatie, bijvoorbeeld informatie die wordt verwerkt op grond van artikel 9 of 13 Wpg. Die artikelen kennen langere verwerkingstermijnen. Omdat er in de BVH geen technisch onderscheid gemaakt kan worden tussen deze wetsartikelen, heeft de politie besloten alle informatie ouder dan vijf jaar 'achter het schot' te zetten. Een zogenoemde *poortwachter* beoordeelt eerst of de informatie terecht achter een schot is geplaatst; als dat niet het geval is, wordt de informatie weer zichtbaar gemaakt. Is de informatie op grond van artikel 8 verwerkt en dus wel terecht achter een schot geplaatst, dan kan deze informatie in een bijzonder geval, voor zover noodzakelijk en met toestemming van het bevoegd gezag, weer beschikbaar worden gesteld.
[34] Op 24 januari 2024 heeft het Kamerlid El Abassi een motie ingediend om registraties met het label 'niet CTER-waardig' in kaart te brengen en te verwijderen (Tweede Kamer, vergaderjaar 2023-2024, 29 628, nr. 1196). Deze motie is verworpen.

bij bepaalde ernstige misdrijven, zoals terroristische misdrijven.[35] De KMar heeft ook toegang tot dit register en kan daar CTER-waardige signalen in registreren. Pas in deze fase wordt het onderzoek gericht op de betrokken persoon of personen in plaats van op de gebeurtenis.

Het themaregister biedt de mogelijkheid om 'zachte' gegevens vast te leggen en bijvoorbeeld ook (persoons)gegevens die de politie van andere landen krijgt. Zo kan de politie een informatiepositie opbouwen over handelingen die kunnen wijzen op het beramen of plegen van terroristische misdrijven en over de personen die daarbij betrokken zijn. *Zachte gegevens* zijn bijvoorbeeld gegevens over met wie de persoon omgaat en lidmaatschap van bepaalde groeperingen of verenigingen. De informatie die wordt verwerkt, wordt verkregen zonder gebruik te maken van een BOB-bevoegdheid (op basis van de Wet bijzondere opsporingsbevoegdheden)[36], dus alleen op basis van openbare bronnen of informatie uit politiesystemen. Ook contacten van CTER-waardige personen kunnen worden opgenomen in het themaregister. Het doel daarvan is te beoordelen of er een netwerk is of ontstaat dat zich bezighoudt met het plegen of beramen van terroristische misdrijven. Deze gegevens worden opgeslagen in een systeem dat SummIT heet. De politie laat weten dat de gegevens in SummIT volgens de Wpg periodiek moeten worden gecontroleerd en uiterlijk vijf jaar na de laatste verwerking worden verwijderd.

In het themaregister CTER staan enkele tienduizenden namen, waarvan het merendeel afkomstig is van berichten of lijsten van buitenlandse diensten (dit hoeven dus geen Nederlandse burgers te zijn). Het is niet zo dat alle personen die zijn vastgelegd in het themaregister CTER ook actief worden gesignaleerd of gemonitord. Integendeel, de politie zegt actief geïnteresseerd te zijn in slechts enige honderden van de opgenomen personen. Die komen, na toetsing door een CTER-intelcel en na afstemming met het bevoegd gezag (het OM) op de zogenoemde afstemmingslijst.

Stap 4: plaatsing op de afstemmingslijst

Definitie van afstemmingslijst: 'De afstemmingslijst omvat alle subjecten waarvan een signaal is binnengekomen dat door de intelcel als CTER-waardig is bestempeld (eventueel op basis van eerdere signalen) en waarvan vervolgens door de intelcel – in overleg met het bevoegd gezag – besloten is deze perso(n)on(en) actief of passief te monitoren gezien zijn/hun zorgelijke activiteiten of uitingen, waarbij er minimaal sprake is van radicaal gedachtegoed[37] of betrokkenheid bij radicale personen, netwerken of ideeën én signalen van afzetten/vervreemding van de westerse samenleving of signalen van ondermijning van de democratische rechtsorde.'

[35] Op grond van artikel 10,1b Wpg kan de politie themaregisters gebruiken om inzicht te krijgen in de betrokkenheid van personen bij bepaalde ernstige misdrijven, zoals mensenhandel en terrorisme. De memorie van toelichting bij de introductie van de themaregisters in de Wpg gaat onder andere in op het doel van themaregisters en de noodzaak om een informatiepositie op te bouwen om doorlopend zicht te krijgen en houden op ontwikkelingen die een ernstige bedreiging van de rechtsorde kunnen vormen, zoals terrorisme, door middel van omvangrijke en op bepaalde personen gerichte gegevensverzameling. Het doel is om in beeld te krijgen in hoeverre die personen betrokken zijn bij handelingen of misdrijven en daarbij worden dus gegevens van veelal nog onverdachte personen vastgelegd.
[36] De Wet bijzondere opsporingsbevoegdheden (BOB) is verankerd in het Wetboek van Strafvordering (titel IVa en V). Ook het bepaalde in titel Vb is van belang, omdat hierin de bijzondere bevoegdheden tot opsporing van terroristische misdrijven zijn geregeld.
[37] Het vanuit een bepaalde overtuiging wederrechtelijk willen afdwingen van maatschappelijke veranderingen of politieke besluitvorming.

Een CTER-intelcel bespreekt met de officier van justitie welke personen vanuit het themaregister op de afstemmingslijst zouden moeten komen. Dit gebeurt aan de hand van de bovenstaande definitie. Deze definitie betreft de laagste categorie van de risico-inschatting, waarover verderop meer. Als die ondergrens niet wordt gehaald, komt een persoon niet op de afstemmingslijst, aldus de politie. De intelcel gebruikt daarvoor de informatie die naar voren is gekomen tijdens haar eerdere onderzoek naar die personen (zie stap 1 t/m 3). Op de afstemmingslijst staan enkele honderden personen die worden gemonitord. Plaatsing op de afstemmingslijst is maatwerk en gebeurt op basis van alle persoonlijke en unieke omstandigheden van de betrokkene. De selectie is volgens de politie bijna niet in een procedure of blauwdruk te vatten, omdat het om veel verschillende aspecten gaat. In elk geval hoeft er geen sprake te zijn van een redelijk vermoeden van een strafbaar feit. Aanwijzingen van terroristische misdrijven zijn voldoende.

De KMar draagt geen personen aan voor opname op de afstemmingslijst, maar kan dit zo nodig wel doen in samenwerking met een intelcel van de politie (bijvoorbeeld als het een medewerker van Defensie betreft).

Risicomodel
Voor alle personen die op de afstemmingslijst zijn geplaatst, maakt de politie een risico-inschatting, door allereerst een risicotaxatiemodel toe te passen.[38] Dit model bevat 43 indicatoren waarmee de CTER-intelcel tot een oordeel kan komen over de mate van radicalisering.[39] De politie benadrukt dat dit model niet werkt op basis van algoritmes en dat er niet automatisch gegevens in worden opgenomen die tot een bepaalde uitkomst leiden. Daarnaast kunnen medewerkers van de intelcel de uiteindelijke uitkomst bijsturen op basis van andere beschikbare informatie en hun professionele oordeel. De uitkomst van dit model zegt iets over de mate van radicalisering en geweldbereidheid van een persoon. Daarnaast bekijkt de intelcel de daadwerkelijke dreiging: is er sprake van bereidheid om geweld te (gaan) gebruiken en zijn er risicoverhogende of -verlagende factoren aanwezig? De risico-inschatting resulteert in een risiconiveau: laag, voorstelbaar, hoog of zeer hoog. Voor alle personen op de afstemmingslijst moet het risiconiveau worden vastgesteld.

De intelcel bespreekt in een periodiek overleg met het OM wie er op de afstemmingslijst moet komen en of het nodig is dat iemand op de lijst blijft staan. Hoe vaak dat overleg plaatsvindt, verschilt per intelcel. Wanneer iemand niet meer voldoet aan de ondergrens van het laagste risiconiveau en bespreking niet meer gerechtvaardigd is, wordt de desbetreffende persoon in overleg met het bevoegd gezag van de afstemmingslijst gehaald. Deze persoon blijft wel in het themaregister staan tot de wettelijke termijn van vijf jaar na de laatste verwerking is verstreken.

Stap 5: maatregelen
Bij de bespreking van de afstemmingslijst overleggen de politie en het OM of het noodzakelijk is om concrete en individuele maatregelen (die binnen de bevoegdheid van deze partijen vallen) te nemen ten aanzien van een persoon. Daarbij kan het bijvoorbeeld gaan om nationale of internationale signalering.[40] Het is afhankelijk van de risico-inschatting (laag, voorstelbaar, hoog of zeer hoog) welke maatregelen worden getroffen. De politie geeft aan dat alle genomen maatregelen per casus maatwerk zijn, omdat elke casus weer anders is. Er zijn twee groepen maatregelen: passief monitoren en actief monitoren. Bij passief monitoren is er geen actieve

[38] De politie zegt over dit model dat het om zeer vertrouwelijke informatie gaat, die niet openbaar gemaakt kan worden. De Nationale ombudsman heeft deze informatie voor het onderzoek wel kunnen inzien.
[39] Eerder was het model enkel gericht op islamitisch radicalisme, maar inmiddels zijn de indicatoren op de lijst dusdanig abstract geformuleerd dat ze ook toepasbaar zijn op andere vormen van radicalisering: islamitisch, links en rechts. Het model is niet van toepassing op bijvoorbeeld milieuextremisme.
[40] Dat kan bij reizen vanuit Nederland hinder veroorzaken.

informatie-inwinning, maar gaat het bijvoorbeeld om toevallige waarnemingen of bevindingen. Dit gebeurt in het kader van de algemene politietaak. Bij actief monitoren is wel sprake van actieve informatie-inwinning, in afstemming met het bevoegd gezag (het OM). Naast actieve of passieve monitoring kan de intelcel ook nog ingrijpendere maatregelen nemen, zoals informatie delen met het buitenland of een signalering doen in het SIS of via Interpol. Hoe ingrijpender de maatregel, des te minder zelfstandige bevoegdheden de politie heeft.[41] De intelcellen leggen beslissingen over opgelegde maatregelen en de motivering daarvan niet altijd secuur vast in het themaregister in SummIT, waardoor het soms lastig is om achteraf na te gaan welke beslissingen er zijn genomen, zo geeft de politie aan.

Voor de KMar geldt dat zij alleen maatregelen neemt tegen personen die direct of indirect een relatie hebben met Defensie, zoals militairen. Dit gaat altijd in overleg met de regionale intelcel van de politie in de regio waar de betrokken militair woont en in overleg met het OM.

4.4 Maatregelen: signaleringen en informatiedeling met andere landen

In het kader van CTER zijn de maatregelen waar burgers in de praktijk het meest last van kunnen hebben signaleringen en informatiedelingen met andere landen. Hieronder staat kort beschreven hoe dit in zijn werk gaat en welke waarborgen er zijn om onrechtmatige internationale informatiedeling te voorkomen.

Afweging bij signaleringen

Onder gezag van het OM en via het Landelijk Internationaal Rechtshulpcentrum (LIRC)[42] kunnen de Nederlandse autoriteiten besluiten dat een internationale signalering van een burger op de (Nederlandse) afstemmingslijst nodig is, ook als er (nog) geen strafrechtelijk onderzoek tegen diegene loopt. De beslissing over een dergelijke signalering wordt per geval genomen, na een individuele afweging. Het OM bekijkt daarbij of een internationale signalering noodzakelijk en proportioneel is. Het OM geeft aan dat het de belangen van de persoon over wie informatie wordt gedeeld afweegt tegen het belang van de informatiedeling, bijvoorbeeld op basis van aanwijzingen dat iemand mogelijk betrokken is bij een terroristisch misdrijf. Signaleringen kunnen worden uitgezet via het SIS en via Interpol.

SIS-signaleringen

Het SIS is een informatie-uitwisselingssysteem voor samenwerking op het gebied van veiligheid en grensbewaking in de landen van de EU waar de Schengenverordening geldt, of die op grond van een verdrag deelnemen.[43]

Uitvaardiging van SIS-signaleringen

Het SIS biedt de mogelijkheid om iemand te signaleren voor onopvallende of gerichte controle, met als doel strafbare feiten te voorkomen en de openbare veiligheid te beschermen. Voorwaarde voor deze signalering is dat er duidelijke aanwijzingen zijn dat die persoon strafbare feiten beraamt of pleegt. Het OM beoordeelt per casus of aan deze voorwaarde is voldaan en of de signalering noodzakelijk en proportioneel is. Connecties van personen voor wie bovengenoemde aanwijzingen bestaan, mogen niet in het SIS worden gesignaleerd, alleen die personen zelf.

[41] De politie werkt altijd onder een bevoegd gezag; afhankelijk van de taak is dat de burgemeester of het OM.
[42] Politiële verzoeken lopen altijd via het LIRC. De reden daarvoor is dat het CTER-politieteam bij het LIRC het overzicht wil houden en een coördinerende rol heeft. Justitiële verzoeken lopen via het lokale IRC (dus via de internationale rechtshulpcentra op de lokale parketten). Een internationale signalering voor aanhouding gebeurt per definitie onder het gezag van de lokale officier van justitie en wordt door het lokale IRC uitgezet. De KMar heeft een eigen IRC.
[43] Zie de uitleg over het Schengen Informatie Systeem op de website van de Europese Commissie.

Vervolgens toetst Bureau SIRENE[44] of de officier van justitie de inhoudelijke toets heeft uitgevoerd. Ook voert Bureau SIRENE een kwaliteitscheck uit op de verzochte signalering. Dit houdt in dat het controleert of de signalering volledig en correct is ingevoerd, dus of de persoonsgegevens kloppen en andere informatie volledig is.[45]

Duur en verwijdering van SIS-signaleringen
Voor signaleringen ter onopvallende controle, onderzoekscontrole of gerichte controle in het SIS geldt een termijn van één jaar. Het kan ook zijn dat iemand voor een kortere termijn wordt gesignaleerd. De bevoegde autoriteiten kunnen de signalering verlengen, maar alleen op basis van een nieuwe, grondige individuele beoordeling en met toestemming van het OM, aldus de politie. Als de signalering niet wordt verlengd, wordt deze automatisch uit het SIS verwijderd. Bureau SIRENE kan de SIS-signalering nog tot één jaar na de verwijdering inzien, mits er communicatie over de signalering is geweest tussen verschillende lidstaten of instanties. Daarna wordt de signalering volledig vernietigd. Dan krijg je geen 'hit' meer bij een zoekopdracht in het SIS. Deze Europese regels zijn bedoeld ter bescherming van burgers.

Soms valt nog wel op andere manieren te achterhalen dat er ooit sprake is geweest van een SIS-signalering, bijvoorbeeld via registraties in de BVH en/of SummIT. In die gevallen kan de politie bij inzageverzoeken wel terughalen dát er een signalering was, maar niet meer waaróm (onderbouwing, toetsing en inhoud). Voor de informatie in de BVH en SummIT gelden de bewaartermijnen van de Wpg, dus die informatie wordt vernietigd zodra de wettelijk gestelde verwerkingstermijn verloopt.

Gevolgen van verwijderde SIS-signaleringen voor burgers
De politie geeft aan dat burgers geen hinder zouden moeten ondervinden van een verwijderde SIS-signalering. In de SIS-verordening staat expliciet dat het verboden is om informatie uit het SIS over te nemen in nationale databases en langer te bewaren. Wat volgens de politie niet valt uit te sluiten, is dat SIS-signaleringen voor andere landen aanleiding kunnen zijn om hun eigen informatiepositie over personen die al in de belangstelling staan van hun nationale opsporingsdiensten, verder uit te bouwen. Lidstaten kunnen besluiten deze persoon zelf ook beter in de gaten te gaan houden en zelf een onderzoek starten, of een nationale signalering of aandachtsvestiging in hun landelijke systeem zetten. Dan is de SIS-signalering dus op enig moment verwijderd, maar blijven de autoriteiten in die landen de desbetreffende burger op grond van eigen wetgeving en bevoegdheden alsnog in de gaten houden. Maar dat gebeurt alleen als daar ook echt een reden voor is, dus op basis van bijkomende en opvallende gedragingen; gedrag dat extra is gaan opvallen door de SIS-signalering, zo stelt de politie. Op die manier kunnen mensen nog hinder ondervinden bij het reizen, ook al is de signalering inmiddels uit het SIS verwijderd. Verder kan informatie volgens de politie bewaard blijven als landen mutaties naar aanleiding van de hit met de persoon in hun eigen systeem registreren, bijvoorbeeld als een gesignaleerd persoon de grens passeert. Op die manier komt de mutatie ook in het nationale systeem van dat land te staan. Dit wordt expliciet genoemd en toegestaan in artikel 64 van Verordening (EU) 2018/1862. Hoelang deze informatie bewaard blijft, hangt af van de bewaartermijnen van dat land.

Signaleringen voor derde landen via Interpol
Met een SIS-signalering is iemand in het gehele Schengengebied gesignaleerd. Als het nodig blijkt iemand te signaleren in een derde land, dus buiten het Schengengebied, dan moet dat via

[44] Bureau SIRENE (Supplementary Information Request at the National Entry) is een onderdeel binnen de politie dat belast is met het gegevensbeheer van het Nationaal Schengen Informatie Systeem en is ondergebracht bij het LIRC.
[45] De informatie moet juist zijn en de verantwoordelijkheid daarvoor ligt bij de invoerende intelcel. Daarvoor zijn Schengen-coördinatoren aangewezen. Daarnaast geldt er een zes-ogenprincipe met regionale eenheden en Bureau SIRENE. Ook is er een e-learning ontwikkeld voor gebruikers van het systeem, aldus de politie.

Interpol gebeuren.[46] Ook voor Interpol-signaleringen gelden bepaalde criteria. Die zijn opgenomen in Interpol's Rules on the Processing of Data (RPD).[47] Volgens de wet blijven Interpol-signaleringen vijf jaar geldig, tenzij anders gespecificeerd door het signalerende land. Om de vijf jaar verzoekt Interpol aan het signalerende land om te toetsen of de signalering wel of niet verlengd moet worden. Als dit land besluit de Interpol-signalering niet te verlengen, verwijdert de secretaris-generaal van Interpol die uit haar mondiale politiecommunicatiesysteem. Alle landen waarvoor de signalering zichtbaar was, ontvangen hiervan bericht. Gelet op de soevereiniteit van de lidstaten is het aan de landen zelf om op basis van dit bericht de signalering uit hun eigen nationale systemen te verwijderen, aldus de politie.

Internationale informatiedeling
Volgens de Wpg (artikel 15a, 17 en 17a) is de politie de verwerkingsverantwoordelijke instantie voor het delen van informatie met andere landen binnen of buiten de EU.[48] Nederland kan informatie over personen met het buitenland delen om zelf een betere informatiepositie op te bouwen. Er is dan sprake van politiële informatie-uitwisseling (politie-politie), waarin het OM in principe geen rol speelt. Bij een strafrechtelijke verdenking speelt het OM wel een rol: het toetst of de strafvordering door de informatie-uitwisseling zou kunnen worden belemmerd, zo geeft het OM aan.

Bij informatiedeling door de politie op grond van de Wpg moet de politie zelf als verwerkingsverantwoordelijke toetsen of de informatiedeling rechtmatig is. Het basiskader voor het delen van politiegegevens is artikel 15a Wpg voor het delen met andere EU-lidstaten en artikel 17a Wpg voor het delen met niet-EU-lidstaten (derde landen). Voor derde landen is een extra waarborgtoets vereist, de derdelandentoetsing, om de proportionaliteit en de subsidiariteit van de verstrekking te beoordelen en een afweging te maken tussen de (privacy)belangen van de betrokkene en het belang van opsporing of verstrekking van de betreffende informatie. Een mogelijke schending van de mensenrechten van de betrokkenen wordt daarin meegenomen, zo geeft de politie aan.

Er bestaat een tijdelijke werkinstructie voor de doorgifte van politiegegevens aan derde landen. Die is opgesteld door de Wpg-partijen en het ministerie.[49] Volgens een externe audit over de periode 2019-2022 was er in die periode geen actief toezicht op de naleving van de werkinstructie, waardoor niet duidelijk is welke politiegegevens in die periode zijn doorgegeven aan derde landen.[50] Ook volgt uit de audit dat 'over de verslagperiode onvoldoende is aangetoond dat de wijze van verwerken van persoonsgegevens ten aanzien van betrokkene behoorlijk en rechtmatig is'. In de managementreactie geeft de politie aan dat het interne toezichtstelsel inderdaad moet worden verbeterd.[51]

Een voorbeeld van internationale informatiedeling is de Terrorist Screening Database (TSDB). De VS heeft deze *watchlist* na de aanslagen van 11 september 2001 opgesteld voor de screening van personen die naar de VS willen reizen, om te voorkomen dat mensen die een risico kunnen vormen ongemerkt de VS binnenkomen. De politie controleert deze lijst op relaties met

[46] In beginsel kán Interpol ook worden ingeschakeld voor signaleringen binnen het Schengengebied, maar dat is niet gebruikelijk.
[47] De RPD regelt alle gegevensverwerkingen in het Interpol-informatiesysteem, inclusief de verwerking rond de publicatie en verspreiding van *red notices* (signaleren van voortvluchtigen). Deze regels garanderen de efficiëntie en kwaliteit van de internationale samenwerking tussen de politieautoriteiten via Interpol-kanalen. Daarnaast garanderen ze dat de grondrechten van de individuen die het onderwerp zijn van deze samenwerking, gerespecteerd worden.
[48] Voor de KMar is de verwerkingsverantwoordelijke de Minister van Defensie.
[49] De politie heeft dit stuk openbaar gemaakt naar aanleiding van een Woo-verzoek. Het stuk is gepubliceerd op de website van de politie.
[50] Zie Tweede Kamer, vergaderjaar 2023-2024, 29628 nr. 1190, bijlage 'Nationale Politie Privacy assurancerapport inzake Wet politiegegevens'.
[51] Zie Tweede Kamer, vergaderjaar 2023-2024, 29628 nr. 1190, bijlage 'Managementreactie externe Wpg-audit 2022'.

Nederland, en als daar in het kader van de nationale veiligheidstaken reden voor is, verwerkt zij die informatie in de eigen nationale systemen. De politie deelt ook informatie over personen op de afstemmingslijst met de VS, maar alleen van personen die ouder zijn dan 12 jaar die zijn uitgereisd, teruggekeerd of vermoedelijk overleden, en alleen als voor hen een hoog of zeer hoog risico geldt. Dat wordt per geval afgewogen. Deze lijst wordt twee keer per jaar aan de VS verstrekt. Sinds februari 2021 is in overleg met het OM besloten de namen van personen in de categorieën ‘verijdelde uitreizen’ en ‘potentiële uitreizigers’ niet meer te delen met de VS. Wel deelt de politie de personen op de afstemmingslijst die ouder zijn dan 12 jaar twee keer per jaar met België en Duitsland.

5 Inzage, toezicht en rechtsbescherming

5.1 Inleiding

Wanneer burgers vermoeden dat de (reis)problemen die ze ondervinden worden veroorzaakt doordat er (CTER-gerelateerde) informatie over hen is gedeeld, dan kunnen ze om inzage vragen bij instanties die hier mogelijk bij betrokken waren. Burgers worden bijvoorbeeld op dit spoor gezet doordat ze in het buitenland ondervraagd of geweigerd worden in verband met informatie of een signalering uit Nederland. Via inzage proberen ze te achterhalen welke informatie er over hen is vastgelegd en gedeeld. Hieronder volgt een overzicht van de regelgeving op het gebied van inzageverzoeken. Vervolgens staat beschreven wat de betrokken instanties vertellen over CTER-gerelateerde inzageverzoeken en de manier waarop ze deze behandelen. Verder staat in dit hoofdstuk hoe het toezicht op het CTER-proces is geregeld en welke mogelijkheden burgers hebben om de verwerking van hun persoonsgegevens door de overheid te corrigeren.

5.2 Regelgeving over verzoeken tot inzage en de werkwijze van overheidsinstanties

Hieronder volgt een overzicht van de regelgeving die van toepassing is op verzoeken tot inzage, zowel nationaal als internationaal, en beschrijven de betrokken overheidsinstanties hoe zij inzageverzoeken in de praktijk behandelen.

Regelgeving over verzoeken tot inzage bij politie en KMar

In een Europese richtlijn (Richtlijn (EU) 2016/680) is vastgelegd dat burgers het recht hebben om inzage te vragen in de gegevens die overheidsinstanties (zoals de politie en de KMar) over hen hebben verwerkt en met wie deze gegevens zijn gedeeld (bijvoorbeeld door middel van een signalering). Daarnaast hebben burgers het recht om aanpassing, aanvulling of vernietiging van die gegevens te vragen. Dat kan bijvoorbeeld als de gegevens onjuist of onvolledig zijn of als de gegevens in strijd met een wettelijk voorschrift zijn verwerkt. In hun verzoek moeten ze gemotiveerd uitleggen welke gegevens feitelijk onjuist of onvolledig zijn en aangeven welke gegevens ze gerectificeerd of vernietigd dan wel aangevuld willen hebben. In de Wpg is dit verder uitgewerkt voor de politiegegevens die de politie en de KMar verwerken (artikel 25-28 Wpg).[52] Voor de gegevens die bijvoorbeeld de NCTV verwerkt (in het kader van de bevoegdheden van de NCTV), geldt dat burgers op grond van de AVG om inzage en verwijdering kunnen vragen.

Een verzoek tot inzage, aanpassing of verwijdering wordt volgens de Wpg geweigerd als er sprake is van een uitzonderingsgrond, bijvoorbeeld als er nadelige gevolgen zijn voor de opsporing of vervolging en voor de bescherming van andere personen of de nationale veiligheid (zie voor alle gronden artikel 27 Wpg). Een afwijzing van een verzoek moet schriftelijk worden gemotiveerd. Ook bij AVG-verzoeken geldt dat er weigeringsgronden zijn en dat een afwijzing moet worden gemotiveerd. Burgers kunnen naar de bestuursrechter gaan als ze het niet eens zijn met het besluit op hun verzoek tot inzage of verwijdering. Ook kunnen ze de AP vragen te bemiddelen of te adviseren (artikel 29 Wpg). In dat geval wordt de termijn om naar de rechter te gaan opgeschort, zodat de betrokkene na de bemiddelingspoging alsnog naar de rechter kan. En tot slot kunnen burgers ook een klacht indienen bij de AP als ze denken dat de verwerking van hun persoonsgegevens onrechtmatig is (geweest).

[52] Verwerking is een breed begrip en omvat volgens artikel 1 van de Wpg 'elke bewerking of elk geheel van bewerkingen met betrekking tot politiegegevens of een geheel van politiegegevens, al dan niet uitgevoerd op geautomatiseerde wijze, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen van politiegegevens'. De AVG bevat een soortgelijke definitie voor de verwerking van persoonsgegevens.

Regelgeving over verzoeken tot inzage bij het SIS, Europol en Interpol
Als burgers willen weten of hun persoonsgegevens zijn verwerkt in het signaleringssysteem SIS of door Europol of Interpol, kunnen ze daarvoor een inzageverzoek indienen.[53] Via een inzageverzoek bij Nederlandse instanties (zoals de politie) kunnen ze vragen of die daadwerkelijk gegevens hebben gedeeld met Europol of Interpol. Ook kunnen burgers bij Europol of Interpol een inzageverzoek indienen. In het laatste geval kan bijvoorbeeld ook blijken dat Europol of Interpol gegevens heeft verwerkt die niet uit Nederland afkomstig zijn.

- SIS: in de SIS-verordening is geregeld dat mensen een verzoek tot inzage in het SIS kunnen indienen en daarnaast gemotiveerd kunnen vragen om aanpassing of verwijdering van de gegevens. De SIS-verordening verwijst hiervoor naar de rechten die zijn vastgelegd in de AVG en naar Richtlijn (EU) 2016/680. In Nederland kunnen burgers zo'n verzoek indienen bij de Landelijke Eenheid van de politie. Ook hier geldt dat beroep bij de rechter of klachtbehandeling en bemiddeling door de AP mogelijk zijn als burgers het niet eens zijn met het besluit op hun verzoek.
- Europol: Europol signaleert zelf geen personen, maar verwerkt informatie in databanken zoals het Europol Informatiesysteem. Voor informatie-uitwisseling tussen Europol en lidstaten wordt het SIENA-systeem gebruikt. In de praktijk kunnen burgers dergelijke inzageverzoeken alleen rechtstreeks indienen bij Europol. Europol neemt vervolgens een besluit. Als burgers het niet eens zijn met dat besluit, kunnen ze een klacht indienen bij de European Data Protection Supervisor. Daarna kan nog beroep worden ingesteld bij het Hof van Justitie van de EU.
- Interpol: burgers kunnen een verzoek tot inzage, aanpassing of verwijdering van gegevens indienen bij de Commission for the Control of INTERPOL's files. Tegen het besluit op zo'n verzoek kan geen rechtsmiddel worden ingediend. Burgers kunnen alleen om herziening vragen als er sprake is van nieuwe feiten of omstandigheden.

Toelichting van de politie op inzageverzoeken
De afdeling Juridische Zaken is verantwoordelijk voor het afhandelen van inzageverzoeken, en vraagt daarvoor bij de CTER-intelcellen alle informatie op die over iemand is vastgelegd. De intelcel levert alle informatie aan die bij de intelcel bekend is. De afdeling Juridische Zaken bepaalt op basis van juridische gronden welke informatie gedeeld kan worden en welke informatie onder de weigeringsgronden valt. De politie geeft aan dat het soms lastig is om een totaalbeeld van alle informatie te krijgen, omdat de informatie op allerlei plekken en in verschillende systemen binnen de politieorganisatie kan worden geregistreerd. De verschillende onderdelen van de politie hebben niet zonder meer toegang tot elkaars informatie. Dit om de privacy van de betrokkenen te beschermen. Als de medewerker die het inzageverzoek afhandelt niet bij alle mogelijke betrokken afdelingen een informatieverzoek uitzet, kan dit echter nadelig uitpakken voor degene die het verzoek heeft ingediend, aldus de politie.

De politie stelt dat online eenvoudig is te vinden hoe burgers een inzageverzoek kunnen indienen. Voor het SIS kan dat volgens de politie op een gebruiksvriendelijke en laagdrempelige manier door een onlineformulier in te vullen. In andere gevallen moet de burger een brief sturen. Sommige media schetsen het beeld dat het niet altijd duidelijk is waar burgers terechtkunnen voor een inzageverzoek. Dat roept bij de politie de vraag op waarom burgers het formulier niet goed weten te vinden en waarom ze niet altijd bij het juiste loket uitkomen. Het zou volgens de politie helpen als daar meer inzicht in komt, zodat zij daar waar nodig iets aan kan doen.

Inzageverzoeken in de praktijk
De politie geeft aan regelmatig CTER-gerelateerde inzageverzoeken te ontvangen. Intern besteedt de politie extra aandacht aan de beoordeling van deze zaken. Zij werkt daarbij samen

[53] Bijvoorbeeld door reisproblemen en het vermoeden dat dit komt door een internationale signalering.

met regionale eenheden. De politie laat weten dat het ze veel tijd kost om deze zaken te beoordelen, omdat het altijd om maatwerk vraagt. Het zijn immers individuele casussen die individueel beoordeeld moeten worden. Zo kan het lastig zijn om achteraf te achterhalen of iemand in het SIS gesignaleerd heeft gestaan, omdat deze signaleringen op grond van de SIS-verordening na een bepaalde periode worden vernietigd. Bij de beoordeling van het inzageverzoek bekijkt de politie of er sprake is geweest van een signalering en zo ja, of deze rechtmatig was.

Verder geeft de politie aan dat zij een check heeft gedaan op alle actuele signaleringen die de politie heeft ingevoerd. Daarbij is volgens de politie geconstateerd dat het bevoegd gezag in alle tot nu toe bekende gevallen een oordeel heeft gegeven over de signaleringen, dus dat deze via de juiste procedure zijn ingevoerd.

Niet alle informatie kan wettelijk worden gedeeld
De politie kan niet altijd volledige openheid van zaken geven over CTER-verwerkingen en signaleringen, bijvoorbeeld in verband met de nationale veiligheid of omdat dit andere burgers kan raken (zie de eerdergenoemde weigeringsgronden in artikel 27 Wpg). Het kan immers zijn dat de politie in het belang van het onderzoek of vanwege haar informatiepositie niet kan vertellen dat iemand in de gaten wordt gehouden. Informatie uit lopende onderzoeken of over de (weging van de) indicatoren kan zij niet delen, op basis van de Wpg. Er kunnen namelijk wettelijke gronden zijn om burgers geen inzage te verlenen. In het besluit op het inzageverzoek staat dan alleen de weigeringsgrond vermeld en een motivering. Als de politie het nodig vindt en dat mogelijk acht, verwijst zij door naar andere instanties. De politie kan soms wel aangeven of iemand bijvoorbeeld op de afstemmingslijst of de LOP-j-lijst heeft gestaan, maar niet altijd. In het geval van de LOP-j-lijst kan dit alleen als daar bijvoorbeeld een mutatie van terug te vinden is in SummIT.

De oorzaak van problemen achterhalen
Als burgers problemen ondervinden bij het reizen, kan dat volgens de politie allerlei oorzaken hebben. Voor zover de politie dat kan beoordelen, is de oorzaak lang niet altijd gelegen in handelingen van de Nederlandse politie of andere Nederlandse autoriteiten. Het kan zijn dat een ander land over eigen informatie beschikt of een eigen signalering heeft ingevoerd. Of het kan gaan om een SIS-signalering die afkomstig is van de AIVD, en daar geeft de politie geen informatie over of inzage in. Er kan ook sprake zijn van informatie-uitwisseling via de TSDB die andere landen onderling met elkaar hebben gedeeld.

Daarnaast kunnen wettelijke regels over verwerkingstermijnen het in de praktijk lastig maken om te achterhalen wat er in het verleden is gebeurd. Oudere registraties zijn vaak al verwijderd. SIS-signaleringen hebben bijvoorbeeld een bepaalde geldigheidstermijn en worden daarna verwijderd. Ze zijn dan direct voor iedereen onzichtbaar, behalve voor Bureau SIRENE. SIRENE kan de signalering nog historisch bevragen, wat betekent dat de signalering nog wel kan worden teruggezocht. Tot één jaar na de verwijdering is de signalering nog zichtbaar voor SIRENE, mits er ten tijde van de signalering communicatie over is geweest. Als er geen communicatie is geweest, dan is de verwijderde signalering ook voor SIRENE onzichtbaar. Als er communicatie over de signalering is binnengekomen via Outlook (dit kan alleen wanneer een Nederlandse politie- of KMar-medewerker informatie over de signalering heeft doorgestuurd naar SIRENE), dan blijft die informatie drie jaar bewaard. De politie moet dus in de dossiers van burgers gaan zoeken naar aanwijzingen dat er een SIS-signalering is geweest. Dat is niet in alle gevallen meer te achterhalen.

Mocht blijken dat er ten onrechte informatie is gedeeld, dan is de politie volgens de Wpg verplicht om de ontvanger daarvan op de hoogte te stellen.[54]

Toelichting van de KMar op inzageverzoeken
Als de KMar inzageverzoeken ontvangt van burgers, laat de privacyfunctionaris van de KMar naslag doen in de relevante KMar-systemen en bekijkt deze de resultaten van die naslag. Er wordt alleen informatie gedeeld die de KMar heeft verwerkt. Als de KMar weet dat de politie ook informatie heeft verwerkt, dan kan zij doorverwijzen naar de politie. In gevallen waarin de KMar niet weet dat er bij de politie ook informatie staat geregistreerd, kan zij niet doorverwijzen naar de politie. Als er een mogelijk verband is met CTER, wordt de reactie op het inzageverzoek afgestemd met het informatieknooppunt CTER van de KMar. Daarnaast vindt in bepaalde gevallen overleg plaats met de privacyfunctionaris van de politie, als er sprake van is dat de politie de zaak overneemt of andersom. Dan wordt bekeken welke informatie kan worden gedeeld en maken de betrokkenen de afweging of ze een beroep willen doen op de weigeringsgronden uit artikel 27 van de Wpg. Zo nodig verwijst de KMar door naar andere instanties, met name de politie. Wanneer bijvoorbeeld blijkt dat een informatieverzoek niet naar de juiste instantie is gestuurd en dat het om politie-informatie gaat, dan is de KMar verplicht om het verzoek door te sturen naar de politie.

De KMar registreert niet hoeveel inzageverzoeken CTER-gerelateerd zijn. Wel geeft zij aan dat het aantal inzageverzoeken kan toenemen als er bijvoorbeeld in de media aandacht is geweest voor een bepaald onderwerp. De KMar ziet een stijging in het aantal beroepszaken bij de bestuursrechter, omdat burgers niet tevreden zijn met de reactie op hun inzageverzoek. Het is een stijging in algemene zin, niet alleen bij de CTER-gerelateerde zaken. Het kan bijvoorbeeld zijn dat burgers niet geloven dat de verstrekte informatie volledig is of twijfelen aan de rechtmatigheid van de gegevensverwerking.

Toelichting van de NCTV op inzageverzoeken
De NCTV ontvangt ook inzageverzoeken. De redenen voor een inzageverzoek bij de NCTV lopen uiteen. Omdat de AVG burgers niet verplicht om een reden op te geven voor hun inzageverzoek en die redenen dus ook niet geregistreerd hoeven worden, is daar geen informatie over beschikbaar. Het is de NCTV wel bekend dat het in enkele gevallen ging om vragen over een CTER-signalering en of hierover informatie bekend was bij de NCTV. De NCTV benadrukt in dit kader dat de organisatie geen opsporings-, inlichtingen- of veiligheidsdienst is. De NCTV heeft dus ook geen toegang tot databases zoals het SIS en kan ook geen namen invoeren in systemen. De NCTV zegt inzageverzoeken conform de AVG te behandelen en dat binnen de hele organisatie wordt bekeken of persoonsgegevens rechtmatig zijn verwerkt.

Toelichting van het ministerie van BZ op zijn rol
Het ministerie van BZ deelt noch registreert CTER-gerelateerde informatie. Het ministerie behandelt dan ook geen CTER-gerelateerde inzageverzoeken zoals de andere, hierboven beschreven instanties. Wel kunnen burgers die in het buitenland in de problemen komen, bijvoorbeeld omdat hun de toegang tot een (derde) land wordt geweigerd, al dan niet vanwege een vermeende CTER-registratie of vanwege detentie, zich wenden tot de Nederlandse diplomatieke vertegenwoordiging in dat land. Het ministerie kan dan consulaire bijstand verlenen volgens de daarvoor geldende kaders, zoals beschreven in de Staat van het Consulaire.

In eerste instantie kunnen de betrokkenen zelf bij de lokale (grens)autoriteiten navraag doen waarom ze een land niet in mogen. Als een ander land verklaart dat de weigering berust op een signalering door een Nederlandse instantie, kan het ministerie deze persoon verwijzen naar de

[54] Uit de Wpg volgt dat burgers een schadevergoeding kunnen krijgen als ze schade lijden doordat in strijd met de Wpg is gehandeld.

reguliere mogelijkheden van een (Nederlandse) signalerende instantie (bijvoorbeeld de politie of Interpol). Het ministerie geeft aan dat het zelf niets kan betekenen voor de betrokkene en een (onterechte) registratie of signalering waar iemand mogelijk last van heeft niet ongedaan kan maken. Het ministerie van BZ is namelijk geen signalerende instantie. Dat is aan de instantie die de registratie eventueel heeft gedeeld.

Het is ook mogelijk dat iemand noch door een Nederlandse, noch door een buitenlandse instantie internationaal is gesignaleerd. Het kan zijn dat het land in kwestie een nationale rechtsgrond heeft om een Nederlandse burger in het betreffende land te signaleren en daar niets over openbaar maakt, om redenen die aan het land zelf zijn. In dat geval is het handelingsperspectief van het ministerie beperkt. Het ministerie van BZ kan niet interveniëren in de rechtsgang van een ander land. Burgers zijn dan verantwoordelijk voor hun eigen verdediging. Als ze daar niet toe in staat zijn, is het aan het land waar iemand is gedetineerd om voor een advocaat te zorgen. De Nederlandse ambassade kan ter plaatse helpen door de betrokkene in contact te brengen met de relevante buitenlandse instantie aldaar.

Mocht blijken dat er sprake is van stelselmatige weigering, waarbij meerdere Nederlandse burgers om onduidelijke gronden geen toegang krijgen tot een land, dan kan de Nederlandse overheid, via het ministerie van BZ, overwegen om daarover in contact te treden met de instanties van het betreffende land. Wanneer en onder welke omstandigheden dit raadzaam is, verschilt per geval. Hierin speelt ook de bilaterale relatie met het desbetreffende land een rol.

5.3 Toezicht op het CTER-proces

Hieronder beschrijven we hoe het toezicht op het CTER-proces is geregeld.

Toezicht door de AP

De AP is een onafhankelijke overheidsinstantie die toezicht houdt op de naleving van verschillende privacywetten, zoals de AVG en de Wpg. De AP heeft daarom ook een belangrijke rol als het gaat om de verwerking van persoonsgegevens door de politie en de KMar. Het gaat dan zowel om toezicht op individueel niveau (bij bemiddelingsverzoeken en klachten) als op systeemniveau (bijvoorbeeld door structurele onderzoeken te doen naar naleving van de wet). Zo is de AP verantwoordelijk voor het toezicht op de verwerking van persoonsgegevens in het nationale deel van het SIS.[55] [56]

Na de aankondiging van dit onderzoek heeft de AP in een openbare brief aan de Nationale ombudsman haar taken en bevoegdheden omschreven.[57] Daarin geeft de AP aan dat zij de bevoegde toezichthouder is om op te treden in zaken waarin de overheid burgers mogelijk onterecht heeft gesignaleerd. Ook schrijft de AP dat zij de klachten behandelt van burgers die vermoeden dat hun persoonsgegevens onrechtmatig en onbehoorlijk zijn verwerkt en/of met derden zijn gedeeld, dat zij een onderzoek kan starten en dat zij namens slachtoffers kan optreden. De AP geeft aan het lastig te vinden wanneer buitenlandse instanties persoonsgegevens doorgeven aan instanties buiten de EU. De (vervolg)verwerking onttrekt zich dan aan het toezicht van de AP. Als burgers in zo'n geval vermoeden dat hun gegevens

[55] De AP schrijft bijvoorbeeld op 20 december 2023 dat uit onderzoek dat zij in 2021 heeft verricht, blijkt dat de politie in het verleden de wet overtrad bij de verwerking van persoonsgegevens in het SIS (dit hoeft niet om CTER-gerelateerde signaleringen te gaan). De kwaliteit van de signaleringen was niet op orde. Zo ontbrak vaak de schriftelijke motivering van de officier van justitie voor het opnemen van een signalering. Ook had de politie onvoldoende gecontroleerd of het nodig was om signaleringen langer te bewaren. De AP schrijft dat de politie in 2022 een plan heeft opgesteld om de kwaliteit van de signaleringen te verbeteren en de controle op signaleringen op orde te krijgen en dat de politie deze maatregelen in 2023 heeft uitgevoerd. De AP heeft dit gevolgd en heeft geconstateerd dat er voldoende maatregelen zijn genomen en dat de overtredingen zijn beëindigd.
[56] De AP schrijft hierover dat het gaat om de nationale datasystemen die in verbinding staan met het centrale SIS. Elke lidstaat geeft signaleringen door via het eigen nationale systeem.
[57] Deze brief is te vinden op de website van de AP.

onrechtmatig of onbehoorlijk zijn verwerkt, moeten ze zich richten tot de toezichthouder of rechter in het betreffende land. Dat is volgens de AP een extra reden voor politie en justitie om zich bij het doorgeven van informatie te vergewissen van het beschermingsniveau in het betreffende land.

Na ontvangst van de brief van de AP hebben de onderzoekers van de Nationale ombudsman een gesprek gevoerd met medewerkers van de AP. Daarin is het volgende aan de orde gekomen.

De rol van de AP bij bemiddelingsverzoeken en klachten
De AP kan burgers bijstaan bij inzageverzoeken. Als de politie hun verzoek tot inzage weigert, kunnen ze de AP vragen om te bemiddelen. Dat wil zeggen dat de AP als tussenpersoon optreedt om een oplossing te vinden waarmee burgers zijn geholpen. De AP kan de politie om verantwoording vragen wanneer gegevens niet worden verstrekt. De AP heeft toegang tot alle gerubriceerde informatie in het kader van CTER bij de betrokken overheidsinstanties, behalve de veiligheidsdiensten. Als de AP constateert dat er geen geldig beroep op weigeringsgronden kan worden gedaan, dan vraagt de AP de politie om het besluit te heroverwegen. Als de politie dat niet wil, wordt de bemiddeling met de desbetreffende burger afgesloten en informeert de AP deze persoon over de uitkomst. Naast een verzoek om bemiddeling kan de burger ook een klacht indienen bij de AP. Als er eerst bemiddeling heeft plaatsgevonden, heeft de AP vaak al meer duidelijkheid over waar het precies om gaat. Bemiddeling is laagdrempeliger dan een klachtenprocedure. Bij een klacht kan de AP een besluit nemen (bijvoorbeeld dat de weigering van inzage of de verwerking onrechtmatig is).

Doorgaans vermoeden burgers die bij de AP een verzoek of klacht indienen al om welk type signalering het zou kunnen gaan. In sommige gevallen klopt hun vermoeden niet; dan vraagt iemand om bemiddeling bij een SIS-inzageverzoek, maar blijkt er geen SIS-signalering te zijn. Als er toch aanwijzingen zijn dat er persoonsgegevens zijn verwerkt, kan de AP de politie vragen om alle mogelijk relevante systemen te doorzoeken. Op dit moment gebeurt dat nog niet standaard, maar de AP geeft aan te werken aan een aanpak die zowel de principes van *doelbinding* en *dataminimalisatie*[58] als het belang van burgers respecteert.

De rol van de AP nadat gegevens zijn verwijderd
De AP laat weten dat het lastig kan zijn om na te gaan of iemand in het verleden gesignaleerd heeft gestaan in SIS, vanwege het verwijderen van de signaleringen. Als er geen sporen meer te vinden zijn van de aanvankelijke (eerste) verwerking, en die verwerking er wél toe heeft geleid dat die persoonsgegevens een eigen leven zijn gaan leiden, is het moeilijk om vast te stellen waar precies de oorzaak van de problemen ligt en of er sprake is geweest van onrechtmatige gegevensverwerking. De bewaartermijnen kunnen dus tot gevolg hebben dat burgers geen duidelijkheid krijgen. Het kan zo zijn dat gegevens met andere landen zijn gedeeld. Maar wat andere landen daarmee doen, is niet zichtbaar en daarmee niet altijd navolgbaar en controleerbaar. Voor EU-lidstaten geldt dat de AP wel kan achterhalen wat er met de gegevens is gebeurd (als het gaat om SIS-signaleringen) door collega-toezichthouders in de andere lidstaat daarnaar te vragen. Voor derde landen ligt dat anders, daar is geen wettelijke voorziening voor. Om hier iets aan te kunnen doen, zou de wet gewijzigd moeten worden. Het is daarom heel belangrijk dat wat er in het SIS staat, rechtmatig is ingevoerd. De eerste registratie moet goed zijn en er moeten goede afspraken zijn over het verwijderen van gegevens uit het systeem, zo geeft de AP aan.

[58] Doelbinding houdt in dat gegevens alleen met een gerechtvaardigd doel mogen worden verzameld; dat doel moet specifiek zijn en vooraf uitdrukkelijk beschreven. Dataminimalisatie houdt in dat organisaties bij het verwerken van persoonsgegevens uitgaan van het principe 'zo min mogelijk'; er mogen dus niet meer gegevens worden verwerkt dan noodzakelijk om het doel te bereiken.

De rol van de AP in een internationale context
De AP loopt soms tegen grenzen aan bij bemiddelings- en klachtenprocedures. Het kan daarom nodig zijn om op te schalen naar het niveau van het ministerie van JenV om een oplossing te vinden. Bijvoorbeeld als er – aanvankelijk rechtmatig – informatie is gedeeld met derde landen, maar deze gegevens door dat derde land verder zijn verwerkt zonder dat dit bij het aanvankelijke delen van de gegevens de bedoeling was. In dergelijke gevallen heeft de AP niet de bevoegdheid om in te grijpen. De AP laat weten dat in dat geval diplomatie door het ministerie van BZ of tussenkomst van het ministerie van JenV[59] uitkomst kan bieden.

De rol van de AP in de ontwikkeling van systemen en wetgeving
De AP heeft de bevoegdheid om breder te kijken dan alleen naar individuele klachten, bijvoorbeeld door op voorhand mee te kijken of te adviseren bij de ontwikkeling van systemen of wetgeving. Ook kan de AP, bijvoorbeeld op basis van klachten, een onderzoek instellen. Klachten of signalen helpen om goed zicht te krijgen op de problematiek. Over CTER-verwerkingen en signaleringen krijgt de AP echter niet veel bemiddelingsverzoeken of klachten.

Toezicht door de Inspectie JenV
De Inspectie JenV houdt toezicht op de uitvoeringsorganisaties op het terrein van justitie en veiligheid, zoals de politie. Dit doet de Inspectie door de kwaliteit van de taakuitvoering en de naleving van regels en normen te onderzoeken. Het toezicht van de Inspectie heeft als doel om risico's te signaleren en organisaties waar nodig aan te zetten tot verbetering. Binnen het toezichtsgebied Security richt de Inspectie zich onder meer op het thema CTER. Met het toezicht op dit thema wil zij bijdragen aan (onder andere) de bescherming van de maatschappij tegen terrorisme, extremisme en radicalisering, maar ook aan de bescherming van de grondrechten van individuele burgers.[60]

In beroep bij de bestuursrechter of de civiele rechter
Burgers kunnen er ook voor kiezen om naar de rechter te gaan. In de meeste gevallen gaat het dan om een beroep bij de bestuursrechter tegen het besluit op een inzageverzoek. De bestuursrechter beoordeelt het besluit op het verzoek tot inzage, aanpassing of verwijdering van persoonsgegevens en bekijkt dan bijvoorbeeld of de betreffende instantie alle opgevraagde gegevens heeft verstrekt. Het uitgangspunt daarbij is dat – als de instantie heeft meegedeeld dat er niet meer gegevens zijn – de burger aannemelijk moet maken dat er toch meer gegevens zijn verwerkt, tenzij de rechter de stelling van de instantie ongeloofwaardig acht.[61] Verder kan de rechter beoordelen of een instantie terecht een beroep heeft gedaan op de weigeringsgronden uit de Wpg of de AVG. De betreffende instantie kan dan onder geheimhouding stukken verstrekken aan de rechtbank (op grond van artikel 8:29 Awb) waarna de rechter de stukken beoordeelt en bekijkt of de opgevraagde gegevens terecht zijn geweigerd.

Uit enkele gepubliceerde uitspraken over inzageverzoeken[62] valt af te leiden dat het voorkomt dat na het eerste besluit of gedurende de beroepsprocedure alsnog nieuwe informatie naar boven komt bij de betreffende instantie(s). De rechter komt dan tot de conclusie dat het eerdere onderzoek niet volledig is geweest. In andere gevallen concludeert de rechtbank dat de zoekactie wel voldoende zorgvuldig was.[63] In één gepubliceerde uitspraak oordeelde de rechter

[59] Het ministerie van JenV merkt hierover op dat het hier geen specifieke bevoegdheden of juridische grondslag voor heeft. Het diplomatieke verkeer is daarnaast belegd bij het ministerie van BZ.
[60] Zie de website van de Inspectie JenV over het toezichtsdomein Security.
[61] Zie de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 19 januari 2022, ECLI:NL:RVS:2022:148.
[62] Het gaat hier om een relatief klein aantal gepubliceerde uitspraken, dus hier zijn geen algemene of verstrekkende conclusies uit te trekken. Zie bijvoorbeeld ECLI:NL:RBAMS:2023:4908, ECLI:NL:RBZWB:2023:6473.
[63] Zie bijvoorbeeld ECLI:NL:RBAMS:2023:4909, ECLI:NL:RBAMS:2024:140, ECLI:NL:RBDHA:2023:19185 en ECLI:NL:RBDHA:2023:19186.

dat de politie de aanduiding CTER of CTER04 uit mutaties (korte rapportages in het politiesysteem) moest verwijderen.[64]

Burgers kunnen er ook voor kiezen om een procedure te starten bij de civiele rechter. Ze stellen dan (met een vordering) dat de overheid onrechtmatig heeft gehandeld en daarom een schadevergoeding moet betalen.

Toezicht door de CTIVD op de verwerking van persoonsgegevens door de AIVD en de MIVD
De CTIVD houdt toezicht op de rechtmatigheid van het handelen van de AIVD en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD)[65] en behandelt klachten over de AIVD en de MIVD. Vanwege de verantwoordelijkheid die de CTIVD heeft als toezichthouder op de verwerking van gevoelige persoonsgegevens door deze diensten, is het voor dit onderzoek relevant om hier een beeld van te krijgen.

De toezichthoudende rol van de CTIVD betekent onder meer dat zij onderzoek doet en openbare toezichtsrapporten uitbrengt. Daarvoor heeft zij zelfstandig toegang tot alle relevante informatie, systemen en medewerkers van deze instanties. Daarnaast behandelt zij klachten over het (vermeende) handelen van de AIVD en de MIVD.

De CTIVD kan toezicht houden op alle taken en bevoegdheden uit de Wiv 2017, dus ook bij internationale samenwerking en het delen van informatie met (inter)nationale instanties. Het toezicht kan tijdens lopende operaties of activiteiten plaatsvinden, maar ook achteraf. Daarnaast is in mei 2018 de Toetsingscommissie Inzet Bevoegdheden in het leven geroepen, die vooraf toetst of de toestemming van de minister van Binnenlandse Zaken en Koninkrijksrelaties (als het de AIVD betreft) of van Defensie (als het de MIVD betreft) voor de inzet van specifieke bijzondere bevoegdheden rechtmatig is. De CTIVD beoordeelt de verwerving van gegevens, de verwerking en de verwijdering of vernietiging. Verder bekijkt zij hoe de compliance binnen de diensten is geregeld, dus in hoeverre de wet- en regelgeving in het interne beleid is opgenomen en wordt nageleefd. Ook moeten incidenten met gegevensverwerking bij de CTIVD worden gemeld, bijvoorbeeld als de diensten hun bevoegdheid niet juist hebben ingezet (bijvoorbeeld zonder de benodigde toestemming) of als informatie niet (tijdig) is vernietigd. De CTIVD kijkt onder meer naar de kwaliteit en de werking van systemen, processen, procedures en maatregelen in de organisaties van de diensten.

Het toezicht is steeds meer risicogestuurd. Hiervoor kunnen allerlei signalen input vormen. Gesprekken op verschillende niveaus bij de diensten, een verzoek van de Commissie voor de Inlichtingen- en Veiligheidsdiensten, klachten of maatschappelijke vraagstukken, kunnen (mede) vormgeven welke risico's de CTIVD ziet. Volgens de CTIVD is het gebruikelijk om als toezichthouder risicogestuurd te werken. Daarbij kunnen verschillende criteria meewegen, bijvoorbeeld door te kijken waar de inbreuk het grootst is. En mocht er iets fout zijn gegaan bij een dienst, moet vooral worden bekeken hoe dit in de toekomst kan worden voorkomen. Bij toezicht gaat het vaak om de vraag hoe je als toezichthouder alle burgers kunt beschermen en tegelijkertijd de diensten goed hun werk kunt laten doen. Met andere woorden: hoe bewaak je de juiste balans tussen nationale veiligheid en fundamentele rechten?

[64] Zie de uitspraak van 31 juli 2023, ECLI:NL:RBAMS:2023:4908, waarin wordt verwezen naar de niet gepubliceerde uitspraak (AMS 19/2518) waarin dit is bepaald.
[65] De grondslag voor dit toezicht ligt in de Wiv 2017, de Wet veiligheidsonderzoeken en de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma.

Als de AIVD en de MIVD[66] informatie internationaal willen delen, gelden er verschillende toestemmingsniveaus, afhankelijk van de mate van inbreuk op grondrechten en van de risico's. Dat is een keuze van de wetgever. De CTIVD houdt toezicht op de wegingsnotities,[67] waarin de diensten moeten vastleggen welke afwegingen ze maken als ze willen samenwerken met buitenlandse inlichtingen- en/of veiligheidsdiensten, en op concrete situaties waarin informatie met buitenlandse diensten wordt gedeeld.[68] In de wegingsnotities wordt ook de vraag gesteld of er toezicht is in het betreffende land en zo ja, hoe dat is geregeld. De CTIVD houdt geen toezicht op wat andere diensten en landen doen. Voor het delen van informatie met een *risicodienst* (een buitenlandse dienst die niet op alle beoordelingscriteria voor samenwerking voldoende scoort) geldt een hoger toestemmingsniveau: de minister. Als er onterecht informatie wordt gedeeld, valt dit niet zomaar terug te draaien, maar het is wel belangrijk om aan de buitenlandse dienst waarmee persoonsgegevens zijn gedeeld door te geven dat een persoon niet langer de interesse heeft van de Nederlandse diensten. Hoe de buitenlandse dienst daarmee omgaat, valt buiten de invloedssfeer van de AIVD en de MIVD. Het is aan de buitenlandse dienst om actie te ondernemen in zijn eigen systemen en eventueel in eigen land verdere stappen te zetten mocht dat nodig zijn, bijvoorbeeld als de informatie verder zou zijn verstrekt. Volgens de Wiv 2017 zijn de AIVD en de MIVD bij het verstrekken van informatie verplicht de clausule op te nemen dat deze niet zonder toestemming verder mag worden gedeeld: de derdepartijregel. Die moeten de diensten ook meenemen in hun beoordeling van de aard en intensiteit van de samenwerking met een buitenlandse dienst, in de wegingsnotities.

Behalve toezichthouder is de CTIVD volgens de Wiv 2017 ook de tweedelijnsklachtbehandelaar, nadat de betrokken minister een klacht over de AIVD of de MIVD heeft afgedaan. Als een burger een klacht indient bij de CTIVD, dan heeft de CTIVD de bevoegdheid met alle medewerkers van de diensten te spreken en alle informatie in te zien die er eventueel over de betreffende persoon is verwerkt. Zij beoordeelt of er behoorlijk of onbehoorlijk is gehandeld, onder meer aan de hand van de Wiv 2017, de Wet veiligheidsonderzoeken en de behoorlijkheidswijzer van de Nationale ombudsman. De rechtmatigheid van het optreden van de diensten wordt gezien als onderdeel van de behoorlijkheid. De CTIVD mag geen gerubriceerde informatie delen met een klager. Dat betekent dat de klager geen inzicht krijgt in eventueel gerubriceerde informatie over zijn klacht en daarom ook niet te horen krijgt of er wel of niet bevoegdheden tegen hem zijn ingezet. Klagers kunnen er wel op vertrouwen dat de CTIVD als onafhankelijke instantie met toegang tot alle systemen, informatie en medewerkers grondig onderzoek naar hun klacht heeft gedaan en een bindend oordeel geeft, zo nodig met een maatregel erbij, zoals het stopzetten van een bevoegdheid of een operatie of het vernietigen van gegevens.

---

[66] Over het internationaal delen van informatie heeft de CTIVD onder andere de volgende rapporten gepubliceerd: Toezichtsrapport nr. 73 over het verstrekken van persoonsgegevens aan buitenlandse diensten met een verhoogd risicoprofiel door de AIVD en de MIVD | Rapport | CTIVD en Toezichtsrapport 56 over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten.

[67] Zie Toezichtsrapport 60 over de Wegingsnotities van de AIVD en de MIVD voor de internationale samenwerking met de Counter Terrorism Group- en sigint-partners.

[68] In artikel 88 van de Wiv staan vijf criteria aan de hand waarvan de AIVD of MIVD beoordeelt of met een buitenlandse dienst kan worden samengewerkt en wat de aard en intensiteit van de samenwerking kan zijn. Ook met een buitenlandse dienst die niet op alle criteria goed scoort (verhoogd risicoprofiel) kan worden samengewerkt, maar minder vergaand en met mitigerende maatregelen. Het gaat om de volgende vijf criteria:

1. de democratische inbedding van een buitenlandse dienst: wat is zijn wettelijke basis en hoe is de (parlementaire) controle in het land geregeld?
2. de mensenrechtensituatie in een land: zijn er internationale mensenrechtenverdragen getekend en houdt het land – bijvoorbeeld op het gebied van persvrijheid – zich hieraan?
3. professionaliteit en betrouwbaarheid: kunnen de Nederlandse diensten erop vertrouwen dat een dienst professioneel omgaat met informatie? Deze afweging wordt gemaakt op basis van eerdere ervaringen van de AIVD en MIVD en die van andere diensten.
4. wettelijke bevoegdheden en mogelijkheden: wat kan en mag de dienst van een ander land doen in vergelijking met de AIVD en MIVD?
5. niveau van gegevensbescherming: hoe gaat de dienst om met het opslaan en vernietigen van verzamelde gegevens?

6 Conclusies en aanbeveling

6.1 Conclusies

De Nationale ombudsman heeft in dit onderzoek gekeken in hoeverre de betrokken instanties binnen het CTER-proces behoorlijk omgaan met burgers. Hij heeft daarbij concreet aandacht besteed aan de waarborgen in het proces, het toezicht op het proces en de effectiviteit van de rechtsbescherming. Deze drie factoren bepalen of de overheid in deze context behoorlijk handelt. De waarborgen in het proces en het toezicht daarop moeten voldoende tegenwicht bieden aan de plicht van de overheid om het veiligheidsrisico voor de samenleving zo klein mogelijk te maken. De rechten van individuele burgers dienen hierbij in acht te worden genomen.

Op basis van het onderzoek concludeert de ombudsman dat op alle punten die vanuit het burgerperspectief worden genoemd verbetering nodig is. Met name als het gaat om de controleerbaarheid en toetsbaarheid van de beslissingen en afwegingen van de overheid. Ook concludeert de ombudsman dat, alhoewel er na 2018 verbeteringen in het proces zijn doorgevoerd, burgers er nog niet blind op kunnen vertrouwen dat hun individuele rechten en vrijheden voldoende zijn gewaarborgd. Kortom: de overheid verwacht dat burgers vertrouwen hebben in het besluitvormingsproces van het veiligheidssysteem, maar stelt daar onvoldoende tegenover. Het is niet meer dan begrijpelijk dat dit het wantrouwen bij burgers voedt.

De Nationale ombudsman komt concreet tot de volgende conclusies:

- het CTER-proces is complex en ondoorzichtig voor burgers
- te veel nadruk op het veiligheidsdenken vormt risico
- het toezicht is onvoldoende structureel ingevuld
- de rechtsbescherming is niet effectief voor de burger

CTER-proces is complex en ondoorzichtig voor burgers

Voor burgers is het systeem rondom CTER-registraties ondoorgrondelijk; een black box. Burgers weten over het algemeen niet dát ze in beeld zijn en met welke instanties en/of landen informatie over hen wordt gedeeld. De gevolgen kunnen echter groot zijn. Daardoor komt hun recht op privacy onder druk te staan, zonder dat ze daar iets van merken. Burgers weten pas dat er iets aan de hand is, als ze in hun dagelijks leven tegen de gevolgen aanlopen. Ze weten niet wat de oorzaak is en waar ze moeten beginnen met zoeken om daarover duidelijkheid te krijgen. Er kunnen veel verschillende instanties in binnen- en buitenland bij betrokken zijn.

Als burgers (uiteindelijk) denken te weten tot welke instantie ze zich moeten richten en een inzageverzoek doen, dan wordt veel informatie over de verwerking van hun gegevens niet openbaar gemaakt vanwege het doel ervan: de nationale veiligheid. Overheidsinstanties zijn gebonden aan wettelijke voorschriften als ze informatie met burgers willen delen. Ze bevinden zich in een spanningsveld waarin ze – in de communicatie met de buitenwereld – het belang van transparantie en het belang van veiligheid, zowel nationaal als individueel, tegen elkaar moeten afwegen. Dat betekent dat burgers maar in beperkte mate zicht kunnen krijgen op wat er over hen is geregistreerd en gedeeld.

De ombudsman vindt het begrijpelijk dat er vanwege de nationale veiligheid informatie over burgers wordt vastgelegd en gedeeld zonder dat ze dat weten. Als gevolg daarvan zitten er logischerwijs grenzen aan de informatie die daarover aan hen verstrekt kan worden. Juist omdat het systeem zeer complex en niet (volledig) transparant is, moet daar tegenover staan dat de

overheid alles in het werk stelt om ervoor te zorgen dat de waarborgen, het toezicht en de rechtsbescherming robuust zijn georganiseerd. Dat is nu niet het geval.

Te veel nadruk op veiligheidsdenken vormt risico
Het CTER-proces kent waarborgen om te voorkomen dat burgers zomaar op een lijst terechtkomen. Er bestaat echter een risico dat er in het CTER-proces te veel nadruk ligt op het veiligheidsdenken, terwijl er sprake moet zijn van een balans tussen de nationale veiligheid aan de ene kant en individuele mensenrechten aan de andere kant. Het besef dat de afwegingen en keuzes in het CTER-proces grote impact kunnen hebben op de individuele rechten en vrijheden van burgers kan makkelijk op de achtergrond raken doordat de nationale veiligheid prioriteit heeft. Dat geldt niet alleen voor beslissingen over het registreren en signaleren van burgers, maar ook voor beslissingen over het delen van informatie met het buitenland. Uit de verhalen van burgers blijkt dat internationale signalering en informatiedeling met het buitenland de grootste impact hebben op hun individuele rechten en vrijheden. Vooral omdat de overheid weinig grip heeft op informatie nadat die met het buitenland is gedeeld, en op wat die landen daarmee doen.

Wat de ombudsman opviel tijdens de gesprekken met instanties over hun werkwijze en de afwegingen die ze daarbij maken, is dat er niet expliciet is gerefereerd naar een plek in het proces waarin rechten en vrijheden van individuele burgers concreet en expliciet in kaart worden gebracht. Hetzelfde geldt voor de mogelijke impact van een eventuele inbreuk daarop op hun leven. Deze aspecten moeten helder zijn voordat ze kunnen worden afgewogen tegen het belang van de nationale veiligheid. Omdat niet duidelijk is of deze toets standaard plaatsvindt, kan de ombudsman er niet op vertrouwen dat er in iedere casus sprake is van een expliciete afweging tussen nationale veiligheid en individuele mensenrechten. De overheid moet de impact op het leven van burgers expliciet maken in haar beslissingen en een duidelijke plek geven in het proces. Dat helpt om het risico op en de schijn van te veel veiligheidsdenken te verminderen en het draagvlak voor haar beslissingen – en daarmee het vertrouwen in het proces en het handelen van de overheid – te vergroten.

Toezicht onvoldoende structureel ingevuld
Structureel en onafhankelijk toezicht op het CTER-proces is op dit moment te mager georganiseerd. Het proces ontbeert een structurele blik van buiten. Burgers moeten erop kunnen vertrouwen dat de overheid goed omgaat met hun gegevens, belangen en rechten. Onafhankelijk en structureel toezicht is daarvoor een belangrijke voorwaarde. Dat is des te belangrijker als burgers geen weet hebben van de verwerking van hun gegevens, zoals bij CTER-registraties, en deze verwerking bovendien grote gevolgen kan hebben voor hun leven en dat van hun familie. Ook het Europees Hof voor de Rechten van de Mens (EHRM) benadrukt het belang van effectief en onafhankelijk toezicht in enkele arresten over geheime surveillancemaatregelen.[69] Het Hof stelt daarin onder andere dat het extra belangrijk is om adequaat en onafhankelijk toezicht te hebben in de fase van informatieverzameling, wanneer burgers van niets weten. Op dat moment wordt er immers al inbreuk gemaakt op hun privacy.

Het OM is geen toezichthouder, maar is onderdeel van het CTER-proces en vormt daarbinnen een waarborg, omdat het optreedt als bevoegd gezag. Het OM bepaalt samen met de politie welke burgers op de afstemmingslijst worden opgenomen en of het noodzakelijk is om

[69] Zie EHRM 25 mei 2021, Big Brother Watch e.a. tegen het Verenigd Koninkrijk, ECLI:CE:ECHR:2021:0525JUD005817013. Het Hof kent in het kader van geheime surveillancemaatregelen een grote waarde toe aan effectief en onafhankelijk toezicht. In de arresten van het Hof gaat het met name over regelgeving die (potentieel) ongericht vele burgers raakt (bijvoorbeeld door bulkinterceptie van communicatie). De uitgangspunten in deze arresten zijn echter ook relevant in de context van het CTER-proces, nu het hier ook om heimelijke gegevensverzameling gaat waarvan de impact op burgers groot is, en waarbij het dus aankomt op zeer sterke waarborgen en effectief toezicht.

maatregelen te nemen. Er is ook geen andere onafhankelijke instantie die structureel toezicht houdt op systeemniveau en op de processen en de uitvoering daarvan door de politie en de KMar. Het toezicht is vooral achteraf georganiseerd door de Inspectie JenV en de AP. Fouten of tekortkomingen in het proces worden daardoor pas zichtbaar als de gevolgen al hebben plaatsgevonden. Toezichthouders kunnen wel een onderzoek instellen uit eigen beweging. Dat gebeurt echter maar incidenteel. Het toezicht is minder robuust ingericht dan bijvoorbeeld het toezicht door de CTIVD op de veiligheidsdiensten, terwijl het in beide gevallen gaat om het verwerken en zo nodig delen van zeer gevoelige informatie. De ombudsman vindt dat het toezicht op het CTER-proces van dezelfde kwaliteit moet zijn als het toezicht door de CTIVD.

Rechtsbescherming is niet effectief voor de burger
De beslissingen en afwegingen van de betrokken instanties moeten navolgbaar, uitlegbaar en controleerbaar zijn. Burgers hebben een aantal middelen om te achterhalen en controleren wat de overheid over hen heeft vastgelegd en gedeeld. Dat begint meestal met een inzageverzoek. Ze weten echter vaak niet bij welke instantie(s) ze moeten beginnen. En als ze zich dan tot een instantie wenden, kan die alleen informatie verstrekken uit de eigen systemen, terwijl de informatie die burgers nodig hebben ook bij andere instanties kan liggen. Bovendien geven instanties veelal aan dat ze informatie niet kunnen delen in verband met de nationale veiligheid. Het kan ook voorkomen dat informatie al uit de systemen verwijderd is of dat niet (meer) te achterhalen valt of de informatie uit Nederlandse systemen afkomstig is. Ten slotte zijn beslissingen niet altijd secuur vastgelegd, waardoor het soms lastig is om achteraf na te gaan welke beslissingen er zijn genomen en op basis waarvan. Inzageverzoeken van burgers leveren daarom vaak geen volledig beeld op van wat er over hen is vastgelegd en gedeeld en waarom. Ook krijgen burgers in de praktijk geen antwoord op de vraag of een eventuele gegevensdeling of signalering terecht en proportioneel was.

Als inzageverzoeken geen duidelijkheid bieden, dan kunnen burgers in beroep gaan bij de rechter of naar de AP gaan voor bemiddeling of een klachtenprocedure. Burgers benutten de mogelijkheden bij de AP echter nauwelijks, omdat deze procedures voor hen niet voldoende bekend zijn. Hoewel burgers vaker kiezen voor de weg naar de rechter, levert een juridische procedure vaak evenmin duidelijkheid op. Deze procedures beperken zich meestal tot een discussie over welke gegevens er zijn verwerkt. Het gebeurt niet vaak dat burgers een oordeel krijgen over wat er precies is gebeurd en of er voldoende waarborgen in acht zijn genomen. Daarnaast is een rechtsgang ingewikkeld, duur en tijdrovend. Burgers hebben ook de mogelijkheid om een klacht in te dienen bij de Nationale ombudsman, nadat zij hebben geklaagd bij de instantie waar de klacht over gaat. Zoals eerder toegelicht, biedt klachtbehandeling door de ombudsman ook niet altijd een oplossing.

Uit het voorgaande blijkt dat er weliswaar een systeem van rechtsmiddelen is ingericht, maar dat er in de context van CTER allerlei belemmerende factoren zijn: het is een complex systeem met veel mogelijk betrokken nationale en internationale instanties, er zijn grenzen aan de transparantie vanwege het belang van de nationale veiligheid, er gelden bewaartermijnen waardoor niet alle informatie meer te achterhalen valt en niet alles wordt secuur vastgelegd. Daardoor leveren inzageverzoeken weinig duidelijkheid op, en dat speelt weer mee in een eventuele procedure bij de AP of de rechter. De kans dat die wel duidelijkheid verschaffen is dan zeer klein. Burgers weten de weg naar de AP bovendien niet te vinden. Bij elkaar opgeteld maken deze factoren dat de rechtsbescherming in de praktijk niet effectief is. Het lukt burgers niet om antwoord te krijgen op de vraag: wat is er nu eigenlijk gebeurd en mocht dat? Ook niet van een onafhankelijke instantie.

De overheid is bezig met een handreiking voor burgers die problemen ondervinden, waarin zij burgers duidelijkheid wil geven over waar ze met vragen terecht kunnen. Inmiddels heeft de

minister aan de Tweede Kamer laten weten dat deze handreiking bij de beleidsreactie op dit rapport zal worden betrokken.[70] De praktijk zal moeten uitwijzen of de handreiking burgers daadwerkelijk gaat helpen.

6.2 Aanbeveling

De Nationale ombudsman vindt dat het beter kan en beter moet. Daarom beveelt hij de minister van Justitie en Veiligheid aan om, samen met de betrokken instanties, de genoemde tekortkomingen aan te pakken. En concrete verbeteringen te verwezenlijken op de door de ombudsman genoemde knelpunten. Alleen dan kunnen burgers erop vertrouwen dat hun individuele rechten en vrijheden niet naar de achtergrond verdwijnen bij het beschermen van de nationale veiligheid.

[70] Zie Tweede Kamer, vergaderjaar 2023-2024, 29 628, nr. 1220, 5 september 2024.

Bijlage 1: onderzoeksverantwoording

De Nationale ombudsman heeft een kwalitatief onderzoek uitgevoerd naar de wijze waarop de overheid CTER-gerelateerde registraties en signaleringen in systemen vastlegt en deelt met andere instanties in binnen- en buitenland. Ook heeft de ombudsman onderzocht welke problemen burgers hierdoor ondervinden en hoe de overheid met deze burgers omgaat.

Contacten met betrokken partijen
De Nationale ombudsman heeft met de volgende partijen gesprekken gevoerd:

- Advocaten
- Amnesty International
- Autoriteit Persoonsgegevens
- Burgers
- Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten
- Inspectie Justitie en Veiligheid
- Journalist
- Koninklijke Marechaussee
- Ministerie van Buitenlandse Zaken
- Ministerie van Justitie en Veiligheid
- Muslim Rights Watch Nederland
- Nationaal Coördinator Terrorismebestrijding en Veiligheid
- Nationale Politie: de Eenheid Landelijke Opsporing en Interventies, Bureau SIRENE en de staf Korpsleiding
- Openbaar Ministerie
- Wetenschappers van de Universiteit Leiden, de Universiteit van Amsterdam, de Vrije Universiteit en de Hogeschool Utrecht

Onderzoekers van de Nationale ombudsman hebben de meeste van deze partijen één of meerdere keren geïnterviewd. In het najaar van 2023 heeft een ronde van verkennende gesprekken plaatsgevonden en in de periode maart tot en met augustus 2024 vonden de gesprekken voor het onderzoek plaats. Daarnaast heeft de ombudsman schriftelijke vragen voorgelegd, die de partijen hebben beantwoord.

Focus van de interviews
De Nationale ombudsman analyseerde klachten en signalen en ging in gesprek met burgers, advocaten, belangenorganisaties en een journalist om de ervaringen met het CTER-proces vanuit burgers te kunnen beschrijven. Daarbij werd hun gevraagd om te vertellen wat ze hebben meegemaakt en/of hoe ze het handelen van de overheid hebben ervaren.

Daarnaast heeft de ombudsman het proces rondom CTER-registraties en signaleringen in kaart gebracht. Daarvoor hebben de onderzoekers gesprekken gevoerd met de volgende overheidsinstanties: verschillende onderdelen van de Nationale Politie, de KMar, het OM, het ministerie van JenV, de NCTV en het ministerie van BZ. De ombudsman vroeg deze gesprekspartners onder meer wat een behoorlijke behandeling van betrokken burgers zou moeten inhouden, hoe die behandeling er op dit moment in de praktijk uitziet en welke verbeteringen eventueel nodig zijn.

De Nationale ombudsman sprak ook met toezichthoudende instanties: de AP en de Inspectie JenV. De nadruk lag in deze gesprekken op de manier waarop het toezicht op (CTER-gerelateerde) verwerkingen van persoonsgegevens is geregeld. Ook heeft de ombudsman

gesproken met de CTIVD, die overigens géén rol heeft in het toezicht op het CTER-proces bij de politie en de KMar.

Hoor en wederhoor
De onderzoekers hebben van deze interviews verslagen gemaakt en die ter controle voorgelegd aan de geïnterviewden. Vervolgens heeft de ombudsman alle informatie samengevoegd in een verslag van bevindingen, waarop diverse partijen mochten reageren om eventuele onjuistheden te corrigeren en ontbrekende informatie aan te vullen. De Nationale Politie, de KMar, het OM, het ministerie van JenV, de NCTV, het ministerie van BZ en de AP hebben twee keer de gelegenheid gehad om te reageren op de bevindingen. Ook de CTIVD en de AIVD hebben de bevindingen ingezien en hun reactie gegeven. Na verwerking van alle reacties is dit rapport tot stand gekomen.

Literatuuronderzoek
Voor dit onderzoek heeft de Nationale ombudsman wet- en regelgeving, jurisprudentie, beleidsdocumenten, Kamerstukken en mediaberichten bestudeerd. De geraadpleegde bronnen staan vermeld in de voetnoten in dit rapport.

Bijlage 2: juridisch kader gegevensverwerking

Hieronder volgt een beknopte beschrijving van de juridische context waarbinnen het vastleggen en delen van CTER-gerelateerde gegevens zich afspeelt. Deze context biedt inzicht in de bestaande wet- en regelgeving rond CTER op grond waarvan de betrokken instanties opereren.

Handvest grondrechten EU en Verdrag betreffende de werking van de EU
Burgers hebben het recht op gegevensbescherming en inzage in de over hen verzamelde gegevens. Dit is bijvoorbeeld vastgelegd in het Handvest van de grondrechten van de EU. Het recht op bescherming van persoonsgegevens staat ook in het Verdrag betreffende de werking van de EU (artikel 16). Dit recht is verder uitgewerkt in de Algemene verordening gegevensbescherming (Verordening (EU) 2016/679, AVG) en in de Richtlijn gegevensbescherming rechtshandhaving (Richtlijn (EU) 2016/680, RGR). Zowel de AVG als de RGR gelden in de hele EU.

Algemene verordening gegevensbescherming
De AVG gaat over de verwerking van persoonsgegevens in brede zin. Het gaat dan zowel om het verwerken van gegevens door de overheid als door bijvoorbeeld bedrijven. De AVG is rechtstreeks van toepassing in Nederland; burgers kunnen dus op grond van de AVG een verzoek tot inzage indienen bij een organisatie. De AVG kan bijvoorbeeld van toepassing zijn bij mogelijke gegevensverwerkingen door de NCTV. Als burgers vermoeden dat de NCTV hun persoonsgegevens heeft verwerkt, kunnen ze op grond van de AVG een inzageverzoek indienen bij de NCTV.

Richtlijn gegevensbescherming rechtshandhaving
Deze richtlijn gaat specifiek over persoonsgegevens die worden verwerkt ‘met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen’. Als het gaat om politiegegevens is deze richtlijn van toepassing, en niet de AVG. In de richtlijn staan bijvoorbeeld regels voor het verstrekken van persoonsgegevens aan derde landen. Daarnaast staat in deze richtlijn dat burgers het recht hebben op inzage in de verwerkte persoonsgegevens, maar ook dat de overheid de inzage kan beperken (bijvoorbeeld om nadelige gevolgen voor de opsporing te voorkomen of ter bescherming van de nationale veiligheid).

De Richtlijn gegevensbescherming rechtshandhaving is op nationaal niveau uitgewerkt in (onder andere) de Wpg en het daarbij horende Besluit politiegegevens (Bpg). Het verwerken van CTER-registraties door de politie en de KMar valt onder deze regels.

Wet politiegegevens en Besluit politiegegevens
De Wpg is in 2008 in werking getreden (als vervanging van de Wet politieregisters). In deze wet zijn per 1 januari 2019 ook de bepalingen van Richtlijn (EU) 2016/680 verwerkt. De Wpg bevat regels over de verwerking van politiegegevens en de doorgifte of verstrekking daarvan. Daarnaast staan hierin ook de rechten van betrokkenen over inzage en verwijdering van gegevens en regels over rechtsbescherming en toezicht. In het Bpg wordt de Wpg nader uitgewerkt.

Een aantal relevante bepalingen uit de Wpg:

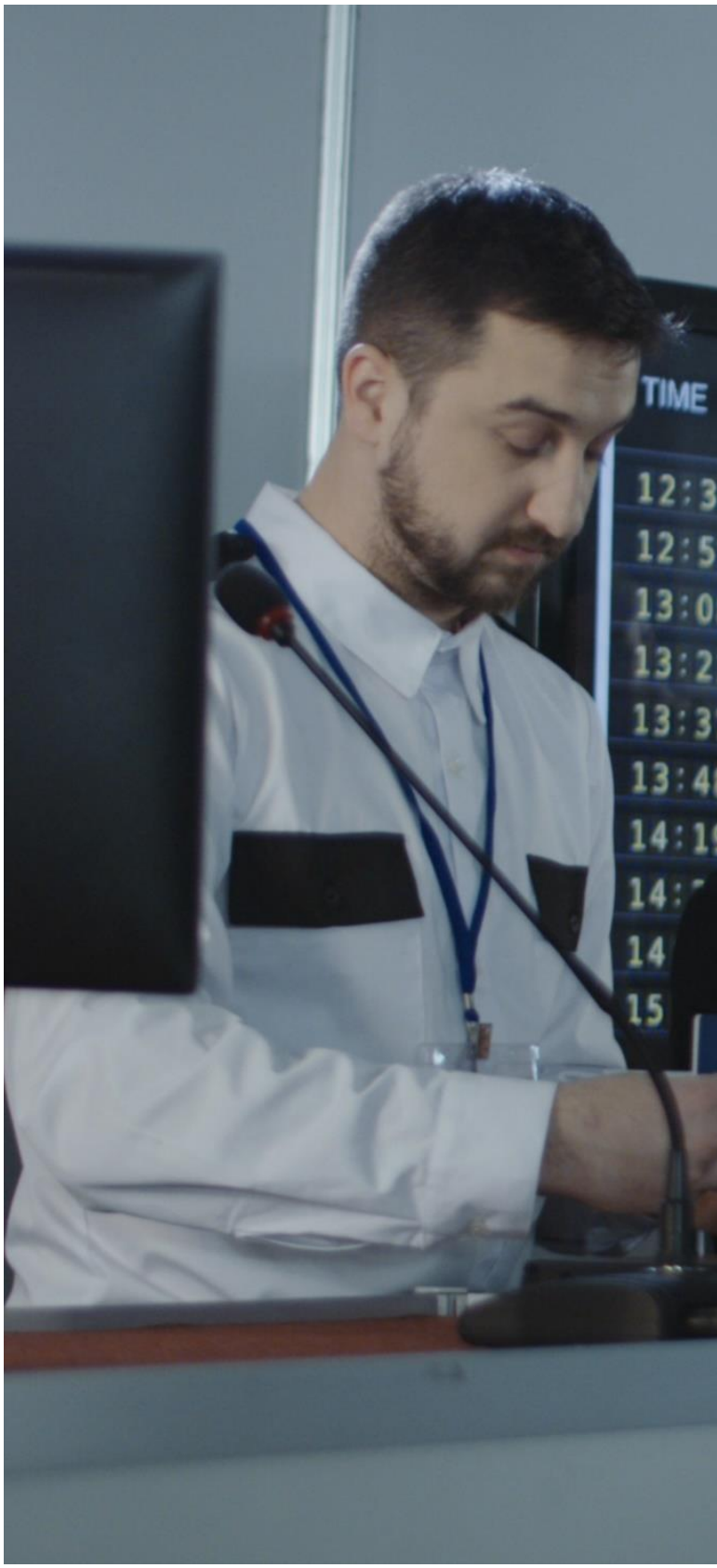
- Er kan een themaregister worden ingesteld om inzicht te krijgen in de betrokkenheid van personen bij ernstige bedreigingen van de rechtsorde, waaronder terrorisme (artikel 10, eerste lid onder b, Wpg en artikel 3:2 Bpg).[71]
- Gegevens die in een themaregister worden verwerkt, worden verwijderd zodra ze niet langer noodzakelijk zijn voor het doel van de verwerking. De gegevens worden uiterlijk vijf jaar na de laatste verwerking van gegevens verwijderd (artikel 10, zesde lid, Wpg).
- Sinds 1 januari 2019 kunnen politiegegevens worden doorgegeven aan instanties in andere EU-lidstaten of aan bepaalde EU-instanties zoals Europol, voor zover deze gegevens nodig zijn voor de voorkoming of opsporing van strafbare feiten (artikel 15a Wpg).[72]
- Sinds 1 januari 2019 kunnen politiegegevens worden doorgegeven aan derde landen of internationale organisaties, als dit noodzakelijk is voor de uitoefening van de politietaak. Dat kan alleen als de Europese Commissie heeft besloten dat er een 'toereikend beschermingsniveau' is of als er andere passende waarborgen zijn. Als die er niet zijn, mag informatie alleen worden gedeeld in uitzonderlijke gevallen, zoals een onmiddellijk en ernstig gevaar voor de openbare veiligheid (artikel 17a lid 3 Wpg).

[71] Als een politieregistratie als 'CTER-waardig' wordt beoordeeld, kan een betrokken persoon worden opgenomen in het themaregister CTER. In hoofdstuk 4 staan het themaregister en de rol van het themaregister in het CTER-proces beschreven.
[72] Politiegegevens kunnen op grond van artikel 16 en 17 van de Wpg ook worden doorgegeven aan gezagsdragers (burgemeesters) en aan inlichtingendiensten.

Bijlage 3: afkortingenlijst

AIVD:	Algemene Inlichtingen- en Veiligheidsdienst
AP:	Autoriteit Persoonsgegevens
AVG:	Algemene verordening gegevensbescherming
Awb:	Algemene wet bestuursrecht
BOB:	Bijzondere opsporingsbevoegdheden
Bpg:	Besluit politiegegevens
BPS:	Bedrijfsprocessensysteem
BVH:	Basisvoorziening Handhaving
BZ:	Ministerie van Buitenlandse Zaken
CTER:	Contraterrorisme, Extremisme en Radicalisering
CTIVD:	Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten
EHRM:	Europees Hof voor de Rechten van de Mens
EVRM:	Europees Verdrag voor de Rechten van de Mens
IRC:	Internationaal Rechtshulp Centrum
JenV:	Ministerie van Justitie en Veiligheid
KMar:	Koninklijke Marechaussee
LIRC:	Landelijk Internationaal Rechtshulpcentrum
LOP-j:	Landelijk Overzicht Politie – Jihadgang
MIVD:	Militaire Inlichtingen- en Veiligheidsdienst
NCTV:	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NTB:	Nationaal Terrorisme Beeld
OM:	Openbaar Ministerie
RGR:	Richtlijn gegevensbescherming rechtshandhaving
RPD:	Rules on the Processing of Data
SIRENE:	Supplementary Information Request at the National Entry

SIS:	Schengen Informatie Systeem
TSDB:	Terrorist Screening Database
VS:	Verenigde Staten
Wiv:	Wet op de inlichtingen- en veiligheidsdiensten
Wpg:	Wet politiegegevens



Nationale ombudsman
Postbus 93122
2509 AC Den Haag

Telefoon 070 356 35 63
nationaleombudsman.nl

Rapportnr: 2024/098 is een uitgave van de Nationale ombudsman, 12 november 2024