over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten

# Deskundigenbericht

# Juridische grondslag multilaterale informatie-uitwisseling

**dr. N.A.N.M. van Eijk**
Nico van Eijk is hoogleraar Informatierecht, in het bijzonder het Media- en Telecommunicatierecht, aan de Faculteit der Rechtsgeleerdheid van de Universiteit van Amsterdam, en directeur van het Instituut voor Informatierecht (IViR). Tevens is hij werkzaam als zelfstandig adviseur.

**Prof. dr. C.M.J. Ryngaert**
Cedric Ryngaert is hoogleraar internationaal recht en programmaleider van de master public international law aan de Universiteit Utrecht. Zijn onderzoek richt zich onder meer op de rechtsmacht van staten en de bescherming van universele waarden.

Utrecht/Amsterdam, september/oktober 2017

# Voorwoord

Dit deskundigenbericht is uitgebracht op verzoek van de CTIVD, die een onderzoek verricht naar de multilaterale gegevensuitwisseling met betrekking tot (vermeende) jihadisten door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). De opstellers van het bericht zijn in de gelegenheid geweest om hierover in diverse fases van de totstandkoming van dit bericht van gedachten te wisselen met de CTIVD.

De CTIVD heeft de opstellers gevraagd een aantal juridische vragen te beantwoorden met betrekking tot de creatie van een specifieke database die in de samenwerking tussen Europese veiligheidsdiensten wordt gebruikt, en waarvan de server zich in Nederland bevindt. Deze vragen zijn in essentie als volgt:

1. Tot welke vorm van verantwoordelijkheid leidt de niet-bindende, informele samenwerking die de veiligheidsdiensten voor ogen hebben?

2. Vallen de individuen wiens gegevens verwerkt worden binnen de rechtsmacht van de participerende staten, d.w.z. hebben deze staten mensenrechtelijke verplichtingen t.a.v. de betrokken individuen?

3. Welke waarborgen m.b.t. de gegevensverwerking in, en het beheer van de database dienen te worden voorzien?

Dit bericht is niet geografisch beperkt: het is relevant voor uitwisseling van gegevens met elke staat, inclusief staten die geen lid zijn van de Europese Unie/Raad van Europa.

Dit bericht gaat methodologisch uit van de huidige juridische stand van zaken in het algemeen internationaal publiekrecht en het internationaal en Europees recht van de mensenrechten (EVRM), met name de doctrines van rechtsmacht en aansprakelijkheid, aangevuld met sectorspecifieke inzichten uit het informatie- en gegevensbeschermingsrecht. Een en ander reflecteert de gezamenlijke deskundigheid van de auteurs van dit bericht.

De auteurs hebben, met name wat betreft de ontwikkeling van het geëigende normatieve kader, ook acht geslagen op de uitgebreide EU-regelgeving en EU-jurisprudentie op het vlak van gegevensbescherming. Formeel is het EU-recht, gezien de uitzondering voor nationale veiligheid echter niet van toepassing op de overdracht van gegevens tussen inlichtingen- en veiligheidsdiensten, althans niet in algemene zin.

Het deskundigenbericht omvat geen uitputtende analyse van de overgelegde vraagstelling, maar beoogt een basis te bieden voor verdere reflectie en verdieping.

# 1. Tot welke vorm van verantwoordelijkheid leidt de niet-bindende, informele samenwerking die de veiligheidsdiensten voor ogen hebben?

De CTIVD stelde de opstellers de vraag hoe het concept 'juridische verantwoordelijkheid' zich verhoudt tot het niet-bindende, informele karakter van de samenwerking tussen de veiligheidsdiensten (*gentlemen's agreements*). Deze vraag impliceert ook de kwestie of juridische bindende afspraken vereist zijn om tot verantwoordelijkheidsafbakening te komen.

Er is geen rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM) met betrekking tot het delen van data en bevoegdheden op basis van informele samenwerkingsverbanden. Het is EVRM-staten niet verboden internationale samenwerking na te streven. Integendeel, internationale samenwerking dient in beginsel een legitiem doel, en het uitgangspunt is dan ook dat internationale samenwerking moet worden aangemoedigd. Uit de relevante rechtspraak van het EHRM blijkt echter dat het staten verboden is een internationale samenwerkingsconstructie zo op te zetten dat individuen het kind van de rekening worden. Om de mensenrechten afdoende te waarborgen dient de internationale samenwerkingsconstructie te voorzien in rechtsbescherming die op zijn minst equivalent is aan de bescherming die normaal wordt geboden door het EVRM.

Wanneer verschillende staten informeel afspraken maken over het delen van gegevens, zal (ingeval geen aparte rechtspersoon wordt opgericht, en geen specifieke afspraken ter zake van verantwoordelijkheid door één of meerdere staten worden gemaakt) de gegevensverwerking in en het beheer van de database in beginsel een *gezamenlijke verantwoordelijkheid* van de participerende staten zijn. In geval van eventuele schendingen kan dit tot gezamenlijke aansprakelijkheid leiden. Het internationaal recht bewaart het stilzwijgen over de precieze aard van *gezamenlijke aansprakelijkheid*, en heeft dus geen specifieke voorkeur voor hoofdelijke aansprakelijkheid. Hierbij dient wel in acht te worden genomen dat hoofdelijke aansprakelijkheid in het nationaal recht werd ontwikkeld om 'zwakkere' partijen tegemoet te komen. Slachtoffers van inbreuken begaan door meerdere partijen, die mogelijk onderling met elkaar verbonden zijn, mogen niet worden benadeeld door de gecompliceerde rechtsverhoudingen die deze partijen onderling hebben. De slachtoffers hebben dan het recht zich voor de gehele schade of in dit geval inbreuk te keren tegen één van deze partijen. Gezien de rationale voor het gebruik van het beginsel van de hoofdelijke aansprakelijkheid – de bescherming van de zwakkere partij – kan worden geargumenteerd dat dit beginsel ook in het recht van de gegevensbescherming aangewezen is. Dit recht beschermt uiteindelijk het *individu*, dat als zwakkere partij t.o.v. de staat, en *a fortiori* t.o.v. meerdere samenwerkende staten, kan gelden.

Een bijzondere zorgplicht geldt voor de staat op wiens grondgebied de (server van de) database zich bevindt. De opstellers begrijpen dat in de voorliggende constructie de AIVD de database beheert. Aangezien Nederland als gaststaat feitelijk een grotere controle en invloed op de gegevensverwerking uitoefenen, zal Nederland ook een uitgebreidere verantwoordelijkheid hebben. Europese rechters zouden kunnen oordelen dat de betrokken diensten als verantwoordelijke of als verwerker in het kader van gegevensbescherming actief zijn, en aldus gebonden zijn aan het gegevensbeschermingsrecht.

## 2. Vallen de individuen wiens gegevens verwerkt worden binnen de rechtsmacht van de participerende staten, d.w.z. hebben deze staten mensenrechtelijke verplichtingen t.a.v. de betrokken individuen?

Overeenkomstig het EVRM-systeem hebben staten slechts mensenrechtelijke verplichtingen t.a.v. individuen, wanneer die laatste binnen de rechtsmacht van de staat vallen (artikel 1 EVRM). In de context van het EVRM gaat de vraag naar rechtsmacht vooraf aan de vraag naar aansprakelijkheid/ verantwoordelijkheid van de staat.

Het EHRM heeft zich nog niet specifiek uitgesproken over de vraag of, en in hoeverre, gegevens die zich bevinden in een gezamenlijke database binnen de rechtsmacht vallen van de staat op wiens grondgebied de server zich bevindt. Uit bestaande jurisprudentie blijkt niettemin dat een inbreuk op privacywaarborgen die zich *territoriaal* afspeelt, binnen de rechtsmacht van de betrokken staat valt. Het heeft daarbij geen belang dat de relevante gegevens personen betreffen die zich buiten het grondgebied bevinden. Een en ander betekent dat inbreuken die betrekking hebben op gegevens die opgeslagen worden in een database die zich op Nederlands grondgebied bevindt, in beginsel binnen de Nederlandse rechtsmacht vallen. Nederland kan zijn verantwoordelijkheid voor eventuele inbreuken wel kwalificeren c.q. beperken door bevoegdheden over te dragen aan, of te delen met andere partijen (zie *supra*). De inbreuken vallen dan nog steeds binnen de rechtsmacht van Nederland, maar de verantwoordelijkheid wordt gedeeld met andere staten. Zoals hoger gesteld, kan Nederland niettemin een bijzondere beheersverantwoordelijkheid hebben die andere staten niet hebben.

Een tweede vraag inzake rechtsmacht is of de gegevens die de deelnemende staten in de database uploaden, ongeacht wat er daarna met deze gegevens gebeurt, binnen de rechtsmacht van de beheerder vallen. De vraag is met andere woorden of Nederland, als potentiële beheerder, verantwoordelijk kan worden gehouden voor de kwaliteit van de door de deelnemende staten aangeleverde gegevens. In beginsel vallen de individuen op wie de gegevens betrekking hebben, niet binnen de rechtsmacht omdat Nederland geen controle over hen uitoefent. Evenwel kan de verantwoordelijkheid van Nederland toch in het gedrang worden gebracht wanneer Nederland toelaat dat 'gecontamineerde' gegevens worden geüpload in de database, en op die manier door andere staten begane schendingen faciliteert. Om verantwoordelijkheid te voorkomen dient Nederland, als beheerder van de database, het uploaden van gegevens door een staat te weigeren wanneer deze kennelijk op onrechtmatige wijze vergaard zijn, of althans dient Nederland zich te onthouden van verdere verwerking of gebruik van deze gegevens in het nationale inlichtingenproces. Het vertrouwensbeginsel dat de gegevensuitwisseling tussen veiligheidsdiensten beheerst, geldt dus niet onverkort. Het wordt gekwalificeerd door een bijzondere zorgplicht.

Een derde vraag inzake rechtsmacht is of gegevens die zich in de database bevinden binnen de rechtsmacht van de andere participerende staten vallen. Voor zover deze staten handelingen stellen m.b.t. gegevens in deze database hebben ze een impact op de personen op wie de gegevens betrekking hebben, en vallen deze personen derhalve binnen hun rechtsmacht. De relevante rechtsmachtstest voor een dergelijke situatie is 'virtuele controle': heeft de staat effectieve controle over de digitale infrastructuur, en dus een impact op de gegevens? Hiervoor werd reeds gesteld dat inbreuken begaan in het kader van een samenwerkingsverband tussen veiligheidsdiensten tot gezamenlijke verantwoordelijkheid kunnen leiden.

## 3. Welke waarborgen m.b.t. de gegevensverwerking in, en het beheer van de database dienen te worden voorzien?

Het gegevensbeschermingsrecht kent een algemeen kader dat met name is neergelegd in het Europees Verdrag voor de Rechten van de Mens (EVRM), in de Conventie 108 van de Raad van Europa en in het Handvest van de Grondrechten van de Europese Unie. De relatie tussen het EVRM en het Handvest is geregeld in artikel 52, lid 3 van het Handvest waarin als volgt is bepaald: '[V]oor zover het handvest rechten bevat die corresponderen met rechten die zijn gegarandeerd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend. Deze bepaling verhindert niet dat het recht van de Unie een ruimere bescherming biedt.' Sectorspecifieke instrumenten zoals de Algemene Verordening Gegevensbescherming (2016/679), de Richtlijn inzake de bescherming van persoonsgegevens die worden verwerkt in het kader van politiële en justitiële activiteiten (2016/680) of de Europol verordening (2016/794) zijn niet van toepassing op de activiteiten van nationale veiligheidsdiensten. Ook Conventie 108 van de Raad van Europa heeft in dit verband maar beperkte betekenis vanwege de daarin opgenomen uitzonderingsgronden.

De algemene bepalingen ten aanzien van gegevensbescherming in de artikelen 7 en 8 van het Handvest en artikel 8 EVRM kennen een rijke jurisprudentie. Uit deze jurisprudentie valt te herleiden dat algemene beginselen van het gegevensbeschermingsrecht relevant blijven binnen de context van nationale veiligheid en mitsdien ook voor multilaterale gegevensuitwisseling, zoals bij de beantwoording van de voorgaande vragen al is geïndiceerd. Deze beginselen, die veelal overeenstemmen met wat bekend staat als 'Fair Information Practices' (FIPs, zoals ontwikkeld binnen het raamwerk van de OECD), zijn eveneens zichtbaar in de genoemde sectorspecifieke regulering die als zodanig nationale veiligheid uitsluit. De toetsing van de Europese Gerechtshoven geeft aan dat in de context van nationale veiligheid, deze beginselen van toepassing zijn en beperkingen daarop dienen te voldoen aan de gebruikelijke proportionaliteitstoetsing.

Het gaat in de context van de onderliggende vraagstelling dan ondermeer om aspecten en randvoorwaarden zoals:

- gegevensverwerking dient gekoppeld te zijn aan een specifiek doel en niet verder te gaan dan noodzakelijk (data-minimalisatie);
- de kwaliteit en veiligheid van de data dient te worden zeker gesteld;
- rechten van data subjecten moeten in acht worden genomen;
- een functionele benadering (bv. waar het gaat om de verantwoordelijkheden voor zowel de verantwoordelijke als de gegevensverwerker);
- het noodzakelijkheids-/proportionaliteitsvereiste richt zich eveneens op elementen zoals bewaartermijnen, de aard van de gegevens (meer of minder gevoelig), subsidiariteit en het inzetten van methoden die 'state of the art' zijn.

In het gegevensbeschermingsrecht wordt bovendien bijzondere nadruk gelegd op onafhankelijk toezicht en transparantie. Gegevensverwerking in het kader van nationale veiligheid zonder toezicht is niet compatibel met de fundamenteel-rechtelijke kaders. Waar de EHRM-jurisprudentie de noodzaak van toezicht zelfstandig heeft ontwikkeld, schrijft het EU-Handvest in artikel 8, lid 3 ten aanzien van gegevensbescherming onafhankelijk toezicht expliciet voor. (Wij laten in het midden of er in deze ook EU-jurisdictie is met betrekking tot nationale veiligheid. Gezien de doorwerking van de EHRM-jurisprudentie via artikel 52, lid 3 EU-Charter is dat niet relevant). Multilaterale informatie-uitwisseling dient derhalve te voldoen aan dezelfde uitgangspunten. Met inachtneming van het bestaande sectorspecifieke recht, ligt het voor de hand om te veronderstellen dat toezichtsverantwoordelijkheden ten aanzien van multilaterale samenwerking langs dezelfde lijnen behoren te lopen teneinde rechterlijke toetsing te kunnen doorstaan.

Aldus vormen de algemene waarborgen in het gegevensbeschermingsrecht die zijn te ontlenen aan de jurisprudentie inclusief zoals deze zijn uitgewerkt in voor nationale veiligheid als zodanig niet geldende regels, richtsnoeren voor de toetsing van gegevensverwerking in een nationale veiligheidscontext. In de literatuur zijn meer uitgebreidere invullingen van de relevante verantwoordelijkheden te vinden.

# 4. Lijst van meest relevante bronnen

## Rechtspraak


Hof van Justitie EU, *Schrems v Data Commissioner*, arrest van 6 oktober 2015, ECLI:EU:C:2015:650

Hof van Justitie EU, *PNR* Canada, Advies 1/15, 26 juli 2017, ECLI:EU:C:2016:656

EHRM, *Al-Skeini and others v. the United Kingdom*, Grand Chamber, Application no. 55721/07, 7 July 2011

EHRM, *Liberty v. United Kingdom*, Application no. 58243/00, 1 July 2008

EHRM, *Bosphorus v Ireland*, Application no. 45036/98, 30 June 2005

EHRM, *Soering v United Kingdom*, Application no. 14038/88, 7 July 1989

EHRM, *Roman Zakharov v. Russia*, Application no. 47143/06, 4 December 2015

EHRM, *Szabó and Vissy v. Hongary*, Application no. 37138/14, 12 January 2016

Internationaal Gerechtshof, *Bosnia Genocide*, Bosnia and Herzegovina v Serbia and Montenegro [2007] ICJ 2

Internationaal Gerechtshof, *Advisory Opinion*, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 9 July 2004

Human Rights Watch Inc. v. The Secretary of State for the Foreign and Commonwealth Office, [2016] UKIPTrib 15_165-CH


## Literatuur


HP Aust, Complicity and the Law of State Responsibility, Cambridge: Cambridge University Press (2011)

F Bignami & G Resta, 'Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance in Community Interests Across International Law' (Eyal Benvenisti & Georg Nolte, eds., Oxford University Press, forthcoming 2017), https://ssrn.com/abstract=3043771

S.Eskens, O. van Daalen en N. van Eijk, '10 Standards for Oversight and Transparency of National Intelligence Services', *Journal of National Security Law & Policy*, Vol. 8 (2016) No. 3, pp.553-594

M Jackson, 'Freeing Soering: The ECHR, State Complicity in Torture, and Jurisdiction', *European Journal of International Law*, Vol. 27 (2016) No. 3, pp 817-830

J.P. Loof, J. Uzman, T. Barkhuysen, A.C. Buyse, J.H. Gerards en R.A. Lawson, *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, Afdeling staats- en bestuursrecht, Universiteit Leiden, augustus 2015

M. Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', *Harvard International Law Journal*, Vol. 56 (2015) No. 1, pp.81-146

VP Tzevelekos, 'Reconstructing the Effective Control Criterion in Extraterritorial Human Rights Breaches: Direct attribution of Wrongfulness, Due Diligence, and Concurrent Responsibility' *Michigan Journal of International Law*, Vol 36:129, (2014) No. 1, pp. 129-178


## Andere


European Commission for democracy through law (Venice Committtee), *Report on the democratic oversight of the security services*, Venice 20-21 maart 2015

EU-Verordening 2016/679 (Algemene Verordening Gegevensbescherming)

EU-Richtlijn 2016/680 (Richtlijn inzake de bescherming van persoonsgegevens die worden verwerkt in het kader van politiële en justitiële activiteiten)

EU-Verordening 2016/794 (Europol)

ILC-artikelen over de Aansprakelijkheid van Staten voor Internationaal Onrechtmatige Daden, *Yearbook of the International Law Commission*, 2001, vol. II, Part Two

OECD, The OECD Privacy Framework, 2013