Appendix IV bij CTIVD rapport no. 56

to the review report on the multilateral exchange of data on (alleged) jihadists by the AIVD

Expert Opinion

Legal basis for multilateral exchange of information

Prof. Dr N.A.N.M. van Eijk
Nico van Eijk is a Professor of Information Law, in particular Media and Telecommunication Law, at the Faculty of Law of the University of Amsterdam, and the director of the Institute for Information Law (Instituut voor Informatierecht, IViR). He also works as an independent advisor.

Prof. Dr C.M.J. Ryngaert
Cedric Ryngaert is a Professor of International Law and the programme leader of the Master of Public International Law at Utrecht University. His research is aimed at the jurisdiction of States and the protection of universal values, among other topics.

Utrecht/Amsterdam, September/October 2017

Preface

This expert opinion has been issued at the request of the Review Committee on the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD), which is performing an investigation into the multilateral exchange of data pertaining to (alleged) jihadists by the General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD). The authors of the expert opinion were given the opportunity to exchange ideas about this matter with the CTIVD in various phases of the preparation of this opinion.

The CTIVD has asked the authors to answer a number of legal questions pertaining to the creation of a specific database used in the cooperation between European security services, and of which the server is located in the Netherlands. These questions are in essence the following:

1. To which standard of responsibility does the non-binding, informal cooperation envisaged by the security services lead?
2. Do the individuals whose data are being processed fall within the jurisdiction of the participating States, i.e. do these States have human rights obligations towards the individuals involved?
3. Which safeguards must be provided for with respect of the data processing in, and the administration of, the database?

This opinion is not geographically limited: it is relevant to the exchange of data with all States, including States that are not members of the European Union/Council of Europe.

Methodologically, this opinion is based on the current legal state of affairs in general international public law and international and European human rights law (ECHR), namely the doctrines of jurisdiction and liability, supplemented with sector-specific insights from information and data protection law. All this reflects the combined expertise of the authors of this expert opinion.

The authors have also given attention to the extensive EU regulations and EU case law with regard to data protection, namely as far as the development of the appropriate normative framework is concerned. However, the EU law, in view of the exception for national security, is not formally applicable to the transfer of data between intelligence and security services, at least not in the general sense.

The expert opinion does not contain an exhaustive analysis of the questions presented, but rather aims at offering a basis for further reflection and in-depth exploration.

1. To which form of responsibility does the non-binding, informal cooperation envisaged by the security services lead?

The CTIVD asked the authors how the concept of 'legal responsibility' relates to the non-binding, informal nature of the cooperation between the security services (gentlemen's agreements). This question also implies the issue of whether legally binding agreements are required to achieve a definition of responsibilities.

There is no case law of the European Court of Human Rights (ECtHR) pertaining to data and power sharing on the basis of informal partnerships. ECHR States are not forbidden from striving for international cooperation. On the contrary, international cooperation serves in principle a legitimate purpose, and the principle is therefore also that international cooperation must be encouraged. However, relevant case law of the ECtHR shows that the States are forbidden from setting up an international cooperation structure so that it adversely affects individuals. To adequately safeguard human rights, the international cooperation structure must provide for legal protection that is at least equivalent—albeit not identical—to the protection normally offered by the ECHR.

When various States make informal agreements about data sharing (if no distinct legal entity is created, and in the absence of specific agreements on responsibility by one or more States), the administration of the database is in principle a *joint responsibility* of the participating States. This can result in *joint liability* in the event of potential violations. International law remains silent on the precise nature of joint liability, and has therefore no specific preference for joint and several liability. However, we do need to take into account in that regard that joint and several liability was developed in national law to accommodate 'weaker' parties. Victims of violations committed by multiple parties, which are potentially mutually linked to each other, cannot be disadvantaged by the complicated legal relationships these parties have with each other. The victims have therefore the right to turn on one of these parties for the full damage or in this case violation. In view of the rationale for the use of the joint and several liability principle – protection of the weaker party – it can be argued that this principle is also appropriate in data protection law. After all, this law protects the individual, who can be considered the weaker party in comparison to the State, and a fortiori in comparison to multiple cooperating States.

A special duty of care applies for the State on whose territory the (server of the) database is located. The authors understand that the AIVD administers the database in the present structure. As the Netherlands actually exercises more significant control and influence on the data processing as the host State, it will also have a more extensive responsibility. European courts could rule that the services involved are active as controllers or as processers in the context of data protection, and are therefore bound by data protection law.

2. Do the individuals whose data are being processed fall within the jurisdiction of the participating States, i.e. do these States have human rights obligations towards the individuals involved?

In accordance with the ECHR system, States have only human rights obligations towards individuals when the latter fall within the jurisdiction of the State (Article 1 of the ECHR). In the context of the ECHR, the question about jurisdiction precedes the question about liability/responsibility of the State.

The ECtHR has not yet specifically given its opinion on the question of, and to what extent, data contained in a common database fall within the jurisdiction of the State on whose territory the server is located. Existing case law nevertheless shows that a violation of privacy safeguards taking place on the territory falls within the jurisdiction of that territory's State. It is not important in that regard that the relevant data pertain to persons situated outside the territory. All this means that violations relating to data stored in a database located on the territory of the Netherlands can in principle fall within the jurisdiction of the Netherlands. The Netherlands can qualify or limit its responsibility for potential violations by transferring powers to, or sharing them with, other parties (supra). In that case, the violations will still fall within the jurisdiction of the Netherlands, but the responsibility is being shared with other States. As stated above, the Netherlands can nevertheless have a special administrative responsibility that other States do not have.

The second question concerning jurisdiction is whether the data uploaded to the database by the participating States fall within the jurisdiction of the administrator, irrespective of what happens to the data afterwards. In other words, the question is whether the Netherlands, as a potential administrator, can be held responsible for the quality of the data supplied by the participating States. In principle, the individuals to whom the data pertain do not fall within the jurisdiction as the Netherlands does not exert control over them. However, the responsibility of the Netherlands can nevertheless be compromised when the Netherlands permits 'contaminated' data to be uploaded to the database, and in this way facilitates violations committed by other States. To prevent responsibility, the Netherlands must, as the administrator of the database, refuse data uploads by a State when these data have manifestly been gathered in an unlawful manner, or the Netherlands must at the least refrain from further processing or using these data intelligence process. Hence, the principle of legitimate expectation that governs the data exchange between security services does not apply unimpaired. It is being qualified by a special duty of care.

The third question pertaining to jurisdiction is whether data in the database fall within the jurisdiction of the other participating States. In so far that these States commit acts in respect of data in this database, they have an impact on persons to whom these data pertain, and these persons therefore fall within their jurisdiction. The relevant jurisdiction test for such a situation of 'virtual control' is: does the State have effective control over the digital infrastructure, and therefore an impact on the data? We have already stated above that violations committed within the context of a partnership between security services can result in joint responsibility.

3. Which safeguards must be provided for with respect of the data processing in, and the administration of, the database?

Data protection law has a general framework that is laid down namely in the European Convention on Human Rights (ECHR), in Convention 108 of the Council of Europe, and in the Charter of fundamental Rights of the European Union. The relationship between the ECHR and the Charter is provided for in Article 52, paragraph 3, of the Charter, in which is provided as follows: 'In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.' Sector-specific instruments such as the General Data Protection Regulation (2016/679), the Directive on the protection of personal data being processed in the context of law enforcement and judicial activities (2016/680) or the Europol Regulation (2016/794) do not apply to the activities of national security services. Convention 108 of the Council of Europe also has limited significance in this context due to the grounds for exception included therein.

The general provisions in respect of data protection in Articles 7 and 8 of the Charter and Article 8 of the ECHR are subject to extensive case law. We can deduct from this case law that general principles of data protection law remain relevant in the context of national security and consequently also for multilateral data exchanges, as has already been indicated in the answers to the preceding questions. These principles, which usually correspond with what is known as 'Fair Information Practices' (FIPs, as developed within the framework of the OECD), are also present in the aforementioned sector-specific regulations that as such exclude national security. The review of European Courts indicates that, in the context of national security, these principles are applicable and limitations thereto must pass the customary test of proportionality.

In the context of the underlying questions, this therefore concerns aspects and preconditions, among others, such as:

- data processing must be linked to a specific purpose and not go further than necessary (data minimisation);
- the quality and security of the data must be safeguarded;
- rights of data subjects must be observed;
- functional approach (e.g. there where it concerns the responsibilities for the responsible party as well as the processer);
- the requirement of necessity/proportionality is also aimed at elements such as retention periods, the nature of the data (more or less sensitive), subsidiarity, and the use of methods that are 'state-of-the-art'.

Moreover, data protection law places a special emphasis on independent oversight and transparency. Data processing in the context of national security without oversight is not compatible with the fundamental law frameworks. While the ECtHR case law has independently developed the need for oversight, the EU Charter explicitly prescribes independent oversight in respect of data protection in Article 8, paragraph 3. (We do not offer an opinion on whether there is also EU case law pertaining to national security. This is not relevant in view of the effect of the ECtHR case law via Article 52, paragraph 3, of the EU Charter). Multilateral information exchange must therefore comply with the same principles. With due regard for the existing sector-specific law, it is reasonable to assume that oversight responsibilities in respect of multilateral cooperation must be along the same lines in order to be able to pass the review of the courts.

Therefore, the general safeguards in data protection law that can be derived from the case law, including those as elaborated in rules not applicable as such to national security, are guidelines for the testing of data processing in the context of national security. More extensive substantiations of the relevant responsibilities can be found in literature.

4. List of most relevant sources

Case law

Court of Justice of European Union, *Schrems v Data Commissioner*, judgment of 6 October 2015, ECLI:EU:C:2015:650

Court of Justice of the European Union, *PNR* Canada, Opinion 1/15, 26 July 2017, ECLI:EU:C:2016:656

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

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

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

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

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

ECtHR, *Szabo and Vissy v. Hungary*, Application no. 37138/14, 12 January 2016

International Court of Justice, *Bosnia Genocide*, Bosnia and Herzegovina v Serbia and Montenegro [2007] ICJ 2

International Court of Justice, *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

Literature

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, and 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, and R.A. Lawson, *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, Afdeling staats-en bestuursrecht, Leiden University, August 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

Other

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

EU Regulation 2016/679 (General Data Protection Regulation)

EU Directive 2016/680 (Directive on the protection of personal data being processed in the context of law enforcement and judicial activities)

EU Regulation 2016/794 (Europol)

ILC Articles on the Responsibility of States for Internationally Wrongful Acts, *Yearbook of the International Law Commission*, 2001, vol. II, Part Two

OECD, The OECD Privacy Framework, 2013