Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU (JUD-IT)
Ensuring Efficient Cross-Border Cooperation and Mutual Trust

Law Enforcement Access to Electronic Data in the framework of Cross-border Criminal Investigations:

State of the Art and Fundamental Rights Challenges

Francesca Galli

JUD-IT State of the Art Report No. 2/October 2018

Abstract

Cross-border law enforcement access to individuals' data held by private companies - profoundly challenge the safeguard of fundamental rights and the rule of law. There are three main models of foreign law enforcement authorities' access to data: (1) mediated access; (2) unmediated access; (3) hybrid access. EU Member States have traditionally privileged the model of mediated access.

The EU has developed a set of data protection clauses and provisions in the realm of law enforcement cooperation, which are crucial to assess the fundamental challenges associated with unmediated access to data. The institutional reform brought by the Lisbon Treaty has placed particular emphasis on the protection of personal data, leading to the coming into force of a new Data Protection Package in

Francesca Gall is Research Associate of the Robert Schuman Centre for Advanced Studies, at the European University Institute and Associate scholar at the Faculty of Law of the University of Maastricht.

This report has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this report are attributable solely to the authors in a personal capacity and not to any institution with which they are associated, nor can they be taken in any way to reflect the views of the European Commission.

Spring 2018. A second set of EU legal standards relates to criminal justice in the form of international agreements, such as bilateral Mutual Legal Assistance agreements, and secondary legislation, most importantly in the Directive on the European Investigation Order.

European courts played a major role: the CJEU intervened to ensure even and consistent interpretation and application of EU law throughout the continent and consequently safeguard EU citizens' rights; the ECtHR welcomed individual challenges to redress situations where rights had been breached and national remedies exhausted.

The Commission recently presented two new proposals on e-evidence which would enable law enforcement authorities to request or compel a third party, *i.e.* a service provider, in another Member State, to disclose personal data about a user, without the request or order having to go through a law enforcement or judicial intermediary in the other Member State.

The EPO proposals witness an additional shift away from traditional MLA agreements, involving the "direct" cooperation between law enforcement authorities seeking to obtain electronic evidence and the foreign service providers in (exclusive) control of it. MLA existing mechanisms are in fact considered lengthy and complex.

Such mechanisms constitute a *de facto* extraterritorial reach of national investigative powers, and an extension of the "sword" function of criminal law via the further privatization of security. The most recent proposals within the EU are deeply influenced by what happens across the Atlantic, most importantly with reference to the Supreme Court Microsoft case and the Cloud Act

Contents

List of abbreviations

AFSJ	Area of freedom, security and justice
CJEU	Court of Justice of the European Union
CLOUD Act	Clarifying Lawful Use of Overseas Data Act
CTC	Counter-Terrorism Coordinator
DPA	Data Protection Authority
DPD	Data Protection Directive
DRD	Data Retention Directive
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EIO	European Investigation Order
EPO	European Patent Office
EPOC	European Production Certificate
EPOC-PR	European Preservation Order Certificate
e-Privacy Directive	Directive on Privacy and Electronic Communications
EU Charter	European Union Charter of Fundamental Rights
FISA	Foreign Intelligence Surveillance Act
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
ISPs	Internet Service Providers
JUD-IT	Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU
MLA	Mutual legal assistance
SCA	Stored Communications Act
TEC	Treaty Establishing the European Community
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Finance Tracking Program

1. Introduction[1]

Given the crucial role played by information technology, the flow of personal data produced and processed by private companies is growing exponentially.

The interest of law enforcement authorities in accessing electronic data has increased proportionally to the growing processing of personal data by private companies. Of course, cross-border law enforcement access to individuals' data held by private companies - in particular when falling outside traditional legal channels of transnational judicial cooperation - profoundly challenges the safeguard of fundamental rights and the rule of law. This report provides an overview and briefly assesses such challenges. The human rights dimension will thus be the backdrop of this research, and a point of reference to rightly assess the compatibility of the law enforcement access to electronic data in the framework of criminal proceedings with the obligation to safeguard the position of suspects within an investigation.

The report focuses on the right to privacy and the protection of personal data as well as defence rights of suspects and defendants in criminal proceedings. In the context of the EU Charter, there are many other rights that are potentially impacted: at least non-discrimination (Article 21 EU Charter), freedom of movement (Article 45 EU Charter), freedom of expression (Article 11 EU Charter), freedom of assembly and of association (Article 12 EU Charter). Yet, privacy and data protection are in this context a good proxy for assessing more general fundamental rights impact across a whole range of rights. Applicable legal instruments and standards (including case-law) under scrutiny encompass the EU and the Council of Europe framework.

In line with the JUD-IT project scope, this Report addresses cross-border judicial cooperation in criminal matters, including both intra-EU cooperation and cooperation with third countries. Transatlantic cooperation is of great interest in this area for a number of reasons.
Both types of cooperation, which are interlinked, are highly dynamic and fundamental rights-sensitive and need to be carefully considered. The same fundamental rights framework under EU law applies to both.

The report first briefly explores models of law enforcement access to personal data, identifying fundamental rights challenges at stake (1). It then provides an overview of how primary and secondary law have evolved to allow cross-border access and exchange data for law enforcement purposes, on the one side, and ensure respect of fundamental rights, on the other side (2). It then addresses the main controversies dealt with by landmark rulings of the CJEU and

[1] This report has been drafted in March 2018 and updated in early June 2018. It thus takes into account legal developments up to that date.

the ECtHR in this context (3). Finally, it elaborates upon current developments either in law or case-law which are likely to further influence the state of the art (4).

2. Law enforcement cooperation: Mediated and unmediated access to personal data

Previous research allowed the identification of three main models of foreign law enforcement authorities' access to data: (1) mediated access; (2) unmediated access (also called remote access claims); (3) hybrid access.[2] EU Member States have traditionally privileged the model of mediated access to authorise the law enforcement access to data in a transnational context.

2.1. The mediated access model

In a **mediated access model,** an authority in the requesting state wishing to obtain access to data under the jurisdiction of another state sends a Mutual Legal Assistance (MLA) request to the designated central authority of that country with recognised competence to order access data transfers from private companies.

There are two important steps: first, the receipt and assessment of the request for access by the designated authority of the requested state that is in charge of examining the MLA request against existing domestic legal requirements and standards; and second, the involvement of an independent judicial authority that validates both the access and the processing of data. During the second step, the designated authority transmits the request to the prosecutor's office to obtain a court order. Once the data are issued, the data are examined against the MLA request, and are then transmitted to the requesting State via the designated MLA channels.

Access to data is thus supervised by the designated authority and an independent court/tribunal of the requested country. Each specific method of mediated access models is regulated by national legal provisions, with a clear difference between adversarial and inquisitorial systems of criminal procedure. In addition, different rules and oversight systems also apply to the issuing of request, depending on the constitutional and institutional framework established in the country concerned. This also applies to the other models.

2.2. The unmediated model

In **unmediated access practices**, an authority in the requesting foreign country communicates its demands directly to the private company holding or controlling the data. This may happen even if the company's decision to disclose the data falls under another jurisdiction and access to the data would entail legal responsibility there. The request does not go through the competent authority responsible to authorise the access to electronic data under MLA and

[2] See Carrera, S.et al. (2015), *Access to Electronic Data by Third- country Law Enforcement Authorities, Challenges to EU Rule of Law and Fundamental Rights*, CEPS, Brussels, section 2.

mutual recognition channels of cooperation (*e.g.* non-content data and voluntary disclosures from service providers).

2.3. The hybrid model

The so-called **'hybrid model'** does not require the authority of the requesting country to transmit its request to an authority in the requested jurisdiction, but to an *ad hoc* authority, not corresponding with a specific state. This authority acts as a special, *sui generis* and non-judicially independent 'mediator'.

The EU has developed this kind of model through the involvement of EU agencies (*e.g.* Europol), responsible for verifying that requests emanating from a third country meet the requirements described in the relevant Agreement. Once this verification has taken place, the data request becomes legally binding under EU law. For instance, the Terrorist Finance Tracking Program (TFTP), an EU-US Agreement on the exchange of financial information, is an attempt by the EU legislator to identify alternative systems to grant law enforcement authorities' access to data across the Atlantic.[3]

With reference to the three models, there are a number of concerns which are worth mentioning. Firstly, one issue is relevant for all models. There is, at least in theory, a fundamental difference between electronic data/information[4], and evidence. In most continental legal systems, for data to be considered "evidence" in criminal procedures, its access, processing and use needs to follow specific provisions to safeguard the rights of the suspect/defendant and pass a legality test by an independent judicial authority. Secondly, the terminology used in mediated access model agreements is at times vague and slippery. The expression "Competent national law enforcement authority" indicates in most Member States police authorities,[5] but important

[3] The signature of the TFTP agreement addresses the media disclosure in 2016 according to which for several years US authorities had been accessing massive amounts of personal data related to European financial transactions by obtaining the information directly from a private company, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), based in Belgium.

[4] The traditional distinction between police and intelligence information is also increasingly blurred. The fact that in many countries there is no distinction as to which kind of information falls within the two different categories or which actors can access and share the information has accentuated such development. This entails an additional layer of complexity in the field of data retention and sharing in the EU Area of Freedom Security and Justice. See Cocq, C. (2017), "'Information' and 'Intelligence': The current divergences between national legal systems and the need for common (European) notions", *NJECL,* 8(3), p. 352.

[5] See Article 2 Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU: "'competent law enforcement authority' [is] a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities". [2006] OJ L 386/89.

distinctions exist among Member States. Intelligence services, covering national security issues, are normally excluded. Another controversial definition is that of "judicial authority". A court of law for the purposes of EU law is characterised by its independence, impartiality and the exclusive interest of applying the rule of law to deliver effective remedies.[6]

The broad interpretation attached to certain definitions is problematic with reference to the safeguard of EU law legal standards when assessing the legality of law enforcement access to data for criminal investigation purposes. This is clearly linked with the need for independent judicial scrutiny. Thirdly, the "unmediated access model" and the "hybrid model" raise several concerns with reference to their compatibility with the rule of law.

The "unmediated access model" lacks consent by the requested state as well as the mediation of an independent judicial authority in the requested state to validate the lawfulness of accessing and processing data. Under this model, a third country may assert the authority under its own national law to access electronic data falling under the scope of EU laws – data which might or might not be stored in EU territory, but which still remains under EU jurisdiction. The risk is to create multiple conflicts of law when, in spite of the requesting country's perception, the transfer of data triggers legal consequences or liabilities in the affected country for the requested private company. Under this model a clear distinction between "data/information" and "evidence" is crucial. In fact, data/information cannot always be considered accurate, reliable and lawful evidence.

The "hybrid access model" raises similar challenges due to the lack of a proper oversight system by an independent judicial authority. It is also affected by accountability and transparency deficits with reference to the decision allowing for access to information.

This State-of-the-Art Report especially focuses on the fundamental right challenges associated to law enforcement authorities' access to data in unmediated access models (as opposed to mediated access models), both within in the EU and between the EU and third-country nationals.

In this context, third-country access to data outside established legal channels of mediated assistance (MLAs) poses a number of fundamental rights challenges, with reference to issues of transfer of jurisdiction (or operations outside own jurisdiction); unclear legal basis; and/or lack of compliance with (EU) data protection rules.

[6] As defined in the EIO Directive. See Directive 2014/41/EU regarding the European Investigation Order in criminal matters, [2014] OJ L130/1.

3. Fundamental rights: overview of EU primary and secondary law

Since the entry into force of the Lisbon Treaty, EU competences have been enhanced and expanded in the field of criminal law. Additionally, given the so-called "Lisbonisation" process, democratic oversight and judicial scrutiny in the EU Area of Freedom Security and Justice (AFSJ) have improved. Firstly, even in this area, the European Parliament is now co-legislator with the Council under the Ordinary Legislative Procedure. Secondly, the CJEU now has full jurisdiction in the AFSJ. Thirdly, the EU Charter of Fundamental Rights has become a legally binding instrument, at the same level as the Treaties, and applicable to all European institutions, agencies and Member States' authorities. The EU has thus developed a set of common rules, including both data protection clauses and provisions in the realm of law enforcement cooperation, which are crucial to assess the fundamental challenges associated to unmediated access to data.

3.1. Privacy and data protection provisions

3.1.1. Primary law

The institutional reform brought by the Lisbon Treaty has placed particular emphasis on the protection of personal data. The right to data protection is now guaranteed in the EU legal order through Article 16 of the Treaty on the Functioning of the European Union (TFEU) - a new horizontal legal basis,[7] Article 36 of the Treaty on the European Union (TEU) and Articles 7 and 8 of the EU Charter of Fundamental Rights of the European Union (EU Charter) at the level of primary law.

Privacy and data protection rights stipulate that personal data can only be collected and retained for specific stated purposes and with the concerned individual's consent according to Articles 7 and 8 of the EU Charter.

Most importantly, the protection of personal data is safeguarded in the EU Charter via an independent right, separate from the right to privacy. There seems to be considerable overlap between the rights to privacy and the protection of personal data.[8] While the right to privacy and the protection of personal data are provided for separately in the EU legal order, Article 8 of

[7] The 1995 Data Protection Directive, in light of the internal market legal basis on which it was adopted, addressed the approximation of national provisions in the private sector most importantly, and only touches on the public sector, the new legal basis provides for a comprehensive protection for all policy areas, including both the internal market and law enforcement.

[8] Lynksey proposes in her monograph that there are three ways to portray the interplay between the rights to privacy and to the protection of personal data: (1) privacy and data protection are complementary tools; (2) Data protection is one component/dimension of the right to privacy; (3) data protection is an autonomous right serving a number of interests, which include but are not limited to privacy. In her view, the model to be favoured is the latter. See Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, OUP, ch. 4.

the European Convention on Human Rights (EHCR) only enshrines a right to privacy (coupled with a number of uncertainties with reference to its scope) and emphasizes the need to protect individuals' private life from the interference of public authorities. Such an approach has a number of shortcomings, particularly in the view of the growing use of information technology.[9] In literature there has been much discussion about the relationship between privacy and data protection.[10] It must be clear though that Article 8 ECHR and the relevant case-law of the Strasbourg Court are and remain crucial for the development of data protection principles.[11]

The scope of the right to data protection as set out by the EU Charter covers all kinds of data (e.g. content, non-content) regardless of their relationship with privacy. Yet its protection of personal data only concerns the processing of personal information, and other aspects of privacy are disregarded. It is noteworthy to highlight that the protection entailed by a combination of the rights to privacy and the protection of personal data in the EU Charter substantially increases the protection of the fundamental right(s) in question.

3.1.2. The 1995 Data Protection Directive and the 2016 Data Protection Package

In addition, three secondary law instruments had (until the recent 2016 data protection reform) set the framework for the protection of personal data: the Data Protection Directive,[12] a Council Framework Decision on processing of data in matters of police and judicial cooperation[13] and the so-called e-Privacy Directive.[14]

---

[9] As argued in the *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 28 January 1981, ETS 108, paragraph 4; and has been one of the underlying motives of *Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector*, and *Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector*.

[10] See e.g. Blok, P.H. (2002), *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht,* PhD dissertation, University of Tilburg, Boom Juridische uitgevers. In the context of law enforcement see Gutwirth, S. and P. De Hert (2007), *"Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power",* in Claes, E. et al (eds.), *Privacy and the Criminal Law*, Intersentia, p. 61-104. With reference to the emergence of data protection as a EU fundamental right see González Fuster, G. (2014), *The emergence of personal data protection as a fundamental right of the EU*, Springer.

[11] See ECtHR, *Klass v. Germany*, Judgment of 6 September 1978, Application No. 5029/71; ECtHR, *Laender v. Sweden*, Judgement of 26 March 1987, Application No. 9248/81; ECtHR, *Segerstedt-Wibergh v. Sweden*, Judgement of 6 June 2006, Application No. 62332/00; ECtHR, *Amann v. Switzerland*, Judgement of 16 February 2000, Application No. 27052/95.

[12] Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, [1995] OJ L 281/31.

[13] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

[14] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, [2002] OJ L 201/37.

In 1995 the European Union adopted a Data Protection Directive (DPD) that set minimum safeguards for Member States to enforce when the processing of personal data is at stake. Subsequently the issue of data protection acquired an entirely new dimension, because of (at least) three legal and societal developments. Firstly, the rise of terrorist attacks in the EU as of 9/11 led to a reconsideration of the value of data protection when the security of the European population is endangered. Secondly, EU law is increasingly implemented through horizontal and vertical cooperation mechanisms between EU and national authorities (and possibly third countries' authorities). This cooperation often entails the sharing of personal and business data. Thirdly, the development of technology and the ongoing digitalization of our economy and society have led to modern communication that primarily entails the processing of data. The possibilities for use and abuse raised further questions on whether the 'traditional' protection of personal data was still adequate.

Building upon the principles encompassed in the Council of Europe Convention 108,[15] and supplementing them with further requirements and conditions, the legal nature of the 1995 DPD necessarily resulted in generally formulated concepts and open standards, leaving broad discretion to Member States regarding its actual implementation process. As a consequence, the instrument led to greater consistency between Member States' data protection provisions, but certainly not to fully consistent solutions in scope and definitions of national provisions, and sometimes resulted in very different versions of the same principles.[16] This lack of consistency in data protection throughout the EU hampered the development of the internal market in a range of areas (including free movement of persons and services) where the processing of personal data plays an increasingly important role. Furthermore, considerable divergences between Member States due to legal traditions or the incorrect implementation and different policy choices when transposing the 1995 DPD hindered the objective of ensuring comparable data protection minimum standards throughout the continent. Challenges resulting from digitalization and globalization and the consequent partial disappearance of borders made the approximation of national data protection provisions even more urgent.

The Commission therefore drafted a new framework for data protection in the EU including two legislative proposals: a proposal for a regulation,[17] setting out a general EU framework for data protection and repealing Directive 95/46/EC; a proposal for a directive on protecting personal

[15] Council of Europe, Convention for the protection of individuals with regards to the automated processing of personal data, Strasbourg 1 October 1985, CETS 108. The Convention, together with OECD guidelines, lays at the heart of EU data protection principles. See OECD Recommendation of the Council concerning guidelines governing the protection of privacy and trans-border flows of personal data, 23 September 1980.

[16] Report from the Commission - First Report on the implementation of the Data Protection Directive (95/46/EC), COM/2003/0265 final.

[17] Proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11 final.

data processed for law enforcement purposes,[18] previously organized under Framework Decision 2008/977/JHA.[19] The two-fold aim of the Regulation is to enhance the level of personal data protection for individuals and to increase business opportunities in the Digital Single Market.[20] The purpose of the Directive is to protect personal data processed for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal offences or the safeguarding against and the prevention of threats to public security. In April 2016 the Regulation and the Directive were adopted, after four years of complex negotiations and intensive lobbying by private companies in Brussels.[21]

A detailed analysis of the content of the two instruments would go beyond the scope of this report. Nevertheless, two questions remain. Firstly, whether the new instruments comply with the purpose behind the reform exercise of having a stronger, more effective, consistent and comprehensive framework in line with the fundamental rights provided under EU primary law, the ECHR, and the Data Protection Convention. Secondly, whether the new instruments meet the stringent requirements established by the CJEU and the ECtHR in their relevant case law (as detailed in the next section on case law developments).

While the Data Protection Package seems to respond to some of the challenges highlighted above, some aspects of the reform certainly leave much to be desired. With regard to the challenges posed by the new technologies and the globalization process, the emerging picture is rather positive. The General Data Protection Regulation (GDPR) aims at adapting the existing data protection framework to better respond to challenges posed by the rapid development of new technologies (particularly online) and increasing globalization, while maintaining the technological neutrality of the legal framework.[22] The GDPR even provides for the monitoring of relevant developments among the duties of each national independent supervisory authority,

[18] Proposal for a directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final.

[19] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, [2008] OJ L 350/60.

[20] Proposal for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11 final, p. 5-6.

[21] Regulation 2016/679/EU of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1; Directive 2016/680/EU of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016] OJ L 119/89.

[22] Hustinx, P. (2017), "EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation" in M. Cremona, *New technologies and EU law,* OUP.

insofar as they have an impact on the protection of personal data, especially the development of information and communication technologies and commercial practices.[23]

With regard to the lack of consistency and the divergences between data protection standards in the EU, the GDPR has significant potential to bring greater uniformity and has been welcomed as a huge step forward towards a more effective and consistent protection of personal data on the continent.[24]
Firstly, given its direct applicability as opposed to the discretion left to Member States through the 1995 DPD, the GDPR avoids problems that come with implementation. Greater consistency will reduce costs for companies operating in different Member States. Furthermore, the GDPR strengthens the roles and powers of key players such as the data subject, the controller (the responsible organization) and the supervisory authorities; their combined intervention may enhance the coherence of the protection of personal data.

Concerning the scope of application, the GDPR closely resembles the existing 1995 DPD that it repeals: it applies to all data processed by automated means (wholly or partly) but it has a wider scope than the 1995 DPD as it applies both in the private and the public sector.[25] In addition it applies to data processing activities of a data controller or a data processor established in the EU; it also applies to data controllers and data processors established outside the EU where their processing activities relate to the offering of goods and services to individuals in the EU or to the monitoring of EU individuals' behaviour.[26] Thus, its scope is broader than the preceding instrument. The 2016 Police Data Protection Directive also has a broader scope, as it applies to both the cross-border processing of personal data as well as the processing of personal data by the police and judicial authorities at purely national level,[27] while previous EU rules applied to the cross-border transfer of personal data only, and this limit has hindered effective cooperation in the field.[28]

Some have argued that the most important shortcoming of the 2016 data protection reform is that it resulted in the adoption of two different instruments, a Regulation and a Directive. This separation seems to be a step backwards with reference to the objective envisaged by Article 16 TFEU – which instead promotes a cross-sectoral approach potentially leading to a comprehensive instrument embracing different policy areas (including the AFSJ) in the same

[23] Ibid, p. 4 and 78.
[24] EDPS Press release, 25 January 2012.
[25] Regulation 2016/679/EU, Article 2.
[26] Ibid., Article 3(2).
[27] Directive 2016/680/EU, Article 1(1).
[28] See Article 1(1), FD 2008/977/JHA.

way.[29] That is a weakness because the level of protection envisaged by the 2016 Police Data Protection Directive is *de facto* lower than in the Regulation. Resulting discrepancies could create a lack of consistency with serious practical consequences especially because data exchanges between private and public entities are increasing.

Finally, as regards transatlantic exchange of personal data, the GDPR maintains the general prohibition of data transfers to countries outside the EU that do not provide an adequate level of data protection.[30] This appears consistent with the *Schrems* judgment (see below for a detailed analysis). However, as a consequence of the requirements set in the CJEU's case law, stricter conditions will apply for obtaining an "adequate" status. EU Model Clauses[31] will remain a useful mechanism to transfer personal data outside the EU. In addition, the GDPR explicitly recognizes and promotes the use of Binding Corporate Rules and codes of conduct as a valid data transfer mechanism.[32]

With a specific reference to the transatlantic dimension, in line with the CJEU's requirements in *Schrems*, the new data protection framework (encompassing both the Privacy Shield and the Umbrella Agreement) provides for strong commitment from the US that no mass surveillance by national security authorities will occur. This would be guaranteed by: strong obligations on companies and enforcement (via supervision mechanisms); clear safeguards and transparency obligations on US government access to data (such as via redress mechanisms provided by an Ombudsman/independent mechanism); and redress for grievances for an effective protection of EU citizens' individual rights.[33]

All in all, therefore, one can conclude that the Data Protection Package has met some of the challenges highlighted while some shortcomings have remained, given the difficulties in finding a common understanding of data protection principles between Member States, EU institutions (including the EU "legislator", EU agencies and the EDPS) and private companies.

EU data protection law as reformed places the consent of the data subject to access or disclosure of personal data at its cornerstones. Consent constitutes a key ground for the

[29] Opinion of the EDPS of 7 March 2012 on the data protection reform package, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/1 2-03-07_EDPS_Reform_package_EN.pdf, p. 49-74.

[30] Regulation 2016/679/EU, Article 45. See T. Bräutigam, "The land of confusion: international data transfers between *Schrems* and the GDPR", in T. Bräutigam and S. Miettinen (eds.), *Data protection, privacy and European regulation in the digital age* (Forum Iuris, 2016).

[31] By virtue of art. 28 GDPR, the European Commission can decide that standard contractual clauses offer sufficient safeguards on data protection for the data to be transferred internationally.

[32] Regulation 2016/679/EU, Article 47.

[33] It is noteworthy to highlight that there are some doubts about the scope of the US Judicial Redress Act which was the condition for the Umbrella Agreement because of the limited scope of protection and excluding third country nationals. See Judicial Redress Act of 2015, 5 U.S.C. § 552a note.

legitimacy and lawfulness of states' interference with the fundamental rights of privacy and data protection. In a law enforcement and criminal justice context, a broader notion of consent translates into the involvement of an independent judicial authority to allow the access and processing of individuals' data.[34] For instance, transatlantic law enforcement unmediated access to data questions the concept of consent most in depth, opening the door to legal uncertainty and arbitrariness.[35] A key source of disagreement between the US and the EU when assessing the legality of access to data and interference with privacy relates to who can give consent to access and share data.

3.1.3. The invalidated Data Retention Directive

The first step towards the establishment of a harmonized data retention framework within the EU was Directive 2006/24/EC (Data Retention Directive)[36]. Grounded on Article 95 TEC (now Article 114 TFEU),[37] the Directive required providers of publicly available electronic communications services or of public communications networks to retain traffic and location data, as well as related data necessary to identify the subscriber or user[38] to ensure that such data is available for the purpose of the investigation, detection and prosecution of serious crime (a concept defined in national law).[39]

Vagueness in the wording of several key concepts in the Directive and its dubious compliance with the rights to privacy and data protection sparked an intense debate between stakeholders and within civil society,[40] and hampered the implementation process of the Directive.[41] The

[34] On the issue of informed consent in the context of the recent scandals of Cambridge Analytica see "The Guardian view on data protection: informed consent needed", *The Guardian*, 19 March 2018 (https://www.theguardian.com/commentisfree/2018/mar/19/the-guardian-view-on-data-protection-informed-consent-needed)

[35] For instance, a key source of disagreement between the US and the EU when assessing the legality of access to data and interference with privacy relates to who can give consent to access and share data.

[36] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, [2006] OJ L 105/54.

[37] Proposal for a directive on the retention of data processed in connection with the provision of public electronic communication services, COM(2005) 438 final.

[38] As defined in Directive 2006/24/EC, Article 2.

[39] Panetta, R. (2013), "The need for harmonized data retention regulation", *E-Commerce Law & Policy*, 15(1).

[40] Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final; Konstadinides, T. (2012), "Destroying democracy on the ground of defending it?" *European Law Review,* 36(5), p.722.

[41] Constitutional courts in Romania (2009), Germany (2010) and Czech Republic (2011) declared the implementing legislation unconstitutional, considering it insufficiently limited circumstances in which data could be accessed, was ambiguous in scope and purpose, and had insufficient safeguards. See Murphy, C. (2010), "Case note on the Decision of the Romanian Constitutional Court of October 2009 on the data retention law", *CMLR,* 47(3), p. 933; Kaiser, A.B. (2010), "German Federal Constitutional Court German Data Retention Provisions Unconstitutional in Their Present Form" *European Constitutional Law Review,* 6(3), p. 503; de Vries, K. et al., "The German

result was a patchwork approximation, where some Member States even widened the scope of application of certain Directive's provision. Firstly, certain Member States extended the access and use of retained data to offences of a less serious nature.[42] Secondly, some national provisions gave intelligence agencies access, thereby allowing use of retained data for preventive purposes. Such provisions potentially enable intelligence services to use data with limited or no judicial or parliamentary oversight and/or review, adding further risk of fundamental rights infringements.[43]

The implementation of the Data Retention Directive proved complex because the data retention framework it entailed was vague and potentially in conflict with privacy and data protection. Eventually, it was invalidated by the CJEU's ruling in *Digital Rights Ireland* (see below for details). This judgment led to disparate reactions among Member States, which mirrored national debates developed during the implementation process.

3.1.4. E-privacy Directive

The predecessor to the Data Retention Directive, the Directive on Privacy and Electronic Communications (e-Privacy Directive) – adopted in 2002 to complement the 1995 DPD for the telecommunications sector – requires traffic and location data to be erased or made anonymous by service providers when no longer needed for the transmission of a communication but still needed for billing or interconnection payments (Articles 5, 6 and 9 e-Privacy Directive).

"Traffic data" are defined as any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Member States, even after the invalidation of the DRD, are still able to restrict this requirement (and thus require telecommunication companies to retain traffic and location data) where necessary, appropriate and proportionate for specific purposes, including safeguarding national security, and preventing, investigating, detecting or prosecuting criminal offences (Article 15 e-Privacy Directive).[44] The provision specifies that to such ends, Member States may adopt laws providing for the retention of data for a limited period of time. Any national measures, however, "shall be in accordance with the general principles of Community law", including fundamental rights.

Constitutional Court Judgment on Data retention: Proportionality Overrides Unlimited Surveillance (Doesn't it?)", in Gutwirth, S. et al (eds.) (2011), *Computers, Privacy and data protection,* Springer, p. 233; EDRi (2011), "Czech Constitutional Court rejects data retention law", *EDRi*; EDRi (2012), "Czech Republic: Attempts to reintroduce data retention", *EDRi*.

[42] *e.g.* Belgium, Italy, the Netherlands, Slovenia and the United Kingdom.

[43] Cocq, C. and F. Galli (2013), *Comparative law paper on data retention regulation in a sample of EU Member States*, SURVEILLE.

[44] National data retention provisions must still comply with the pre-existing Directive 2002/58/EC and in particular with Article 15 once the Data Retention Directive has been considered invalid.

3.1.5. Umbrella agreement & Privacy shield

Two other instruments are worth noticing in the context of transatlantic exchanges. The EU-US **Privacy Shield**,[45] presented on 29 February 2016 to replace the Safe Harbour Decision invalidated by the CJEU in *Schrems*, establishes a data protection framework for transfers of commercial data. Some authors regret the very strong resemblance of this new instrument to the Safe Harbour regime (for example with regard to the self-certification process).[46] Most importantly, mirroring the pre-existing framework under the Safe Harbour Agreement is the general exception of national security, public interest or law enforcement. It is thus still doubtful whether the new regime is satisfactory in light of the CJEU's recent case law. The terrorist attacks in 2015 and at the beginning of 2016 could have once again pushed EU policy makers towards enhancing security at the expense of safeguarding privacy and data protection.[47]

In addition, the EU has concluded and initiated with the US government the so-called **Data Protection Umbrella Agreement** to ensure a high level of protection of personal data transferred between the EU and the US for the prevention, detection, investigation and prosecution of criminal offences, including terrorism.[48] However, some authors regret the strong resemblance of the new instruments to pre-existing ones and are sceptical about compliance with CJEU's requirements.[49] A more critical approach is also possible where standards are moving toward the US level instead.

3.2. Police and judicial cooperation

A second set of EU legal standards relates to criminal justice in the form of international agreements and secondary legislation. Title VI of the EU Charter of Fundamental Rights (Justice) provides the basis upon which these instruments need to be interpreted and applied in practice. Of particular significance is Article 47 EU Charter, which provides for a right to an effective remedy and fair trial before a tribunal.[50] The judicial nature of scrutiny finds its foundations in CJEU case law, which has previously considered judicial accountability a general principle of EU

[45] Communication from the Commission to the European Parliament and the Council, Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final.

[46] For an in-depth analysis of novelties and shortcomings enshrined in the privacy field see Vermeulen, G. (2016), "The Paper Shield", in Svantesson, D. and D. Kloza (eds.), *Transatlantic data privacy relationships as a challenge for democracy*, Intersentia.

[47] To place the current debates in a broader context, see Irion, K. (2015), "Accountability unchained: Bulk Data Retention, Pre-emptive Surveillance, and Transatlantic Data Protection", in M. Rotenberg et al (eds.), *Privacy in the Modern Age*, New Press.

[48] See Europa Rapid Press Release, *Questions and Answers on the EU-US data protection "Umbrella agreement"*, 8 September 2015, MEMO/15/5612.

[49] Vermeulen, n. 46.

[50] Aalto, P. et al. (2014), "Article 47 – Right to an Effective Remedy and to a Fair Trial", in Peers, S. et al (eds.), *The EU Charter of Fundamental Rights: A Commentary*, Hart.

law.[51] Effective and open justice, as well as effective judicial scrutiny, thus constitute central components of the EU legal system when assessing the legality and legitimacy of law enforcement authorities' interferences with EU Charter rights.[52] This is the case even when the notion of "national security" is alleged to justify such interference by State authorities.[53] Equally of great significance is Article 49 EU Charter, encompassing the principles of legality and proportionality of criminal offences and penalties.

In the EU context, such legal standards are most importantly enshrined in bilateral Mutual Legal Assistance agreements (2.2.1) and in the Directive on the European Investigation Order (2.2.2).

3.2.1. Mutual Legal Assistance agreements

Among EU Member States

Mutual legal assistance mechanisms among EU Member States are progressively being replaced by mutual recognition instruments. However, one agreement between EU countries is still in place: the Convention on mutual assistance in criminal matters,[54] which strengthens cooperation between judicial, police and customs authorities.[55]

The Convention introduced a new concept, that of compliance with formalities and procedures expressly indicated by the requesting Member State (*forum regit actum*), which is the opposite of the traditional *locus regit actum* principle. Only to the extent that it does not conflict with fundamental principles of their domestic law, there is an obligation on the requested state to execute requests in accordance with the procedures specified in the request by the requesting state. The rationale of the new concept is that the requested procedural and investigative actions are to be regarded as an extra-territorial extension of the criminal investigations or procedures conducted within the *forum* state. The scope of the principle is not just limited to the execution of letters rogatory. The only forms of cooperation to which the *forum regit actum* principle will not apply, are controlled deliveries, covert investigations and cooperation in so-called joint investigation teams.

[51] *Johnston*, Case 222/84, 15 May 1986.
[52] This general right to effective judicial protection is of course relevant to all data protection related issues assessed so far.
[53] Bigo, D. et al. (2014), "National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges", CEPS, Brussels.
[54] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, [2000] *OJ* C 197/1.
[55] See for a comment Vermeulen, G. (2006), "EU conventions enhancing and updating traditional mechanisms for judicial cooperation in criminal matters", *Revue International de Droit Penal,* 77(1), p. 59.

The presence of the defence counsel at the execution of letters rogatory is mandatory. A major novelty is also the obligation for the requested Member State to take maximal account of deadlines set by the requesting Member State.

In the fields of *customs* and *police* co-operation, there was already an important *acquis* in the field of spontaneous information exchange. According to the Convention, the competent authorities of the Member States may, within the limits of their national law and *without a request to that effect*, exchange information relating to criminal or administrative offences, the punishment or handling of which falls within the competence of the receiving authority at the time the information is provided. The providing authority may impose binding conditions on the use of the information by the receiving authority. The new rule intends – among other things – to facilitate the exchange of information that emerges during or before the closure of investigations, unless this would be contrary to the domestic law of the Member State giving the information.

The provisions with regard to the interception of satellite telecommunications were a difficult point during the negotiations of the Convention and made it impossible for a long time to reach final agreement. In fact, the 1959 Council of Europe Convention[56] did not provide for an explicit, adequate legal basis for cooperation in the interception of telecommunications. The main obstacle in reaching a final agreement was the UK's unwillingness to accept that a Member State on whose territory a target is intercepted should be informed where the interception concerned has been authorized by secret services. Ultimately, however, it was agreed that the new rules on interception will only apply to interception orders authorized in the course of criminal investigations.[57] Thus, proactive or administrative interceptions authorized by secret services would indeed not be subject to the obligation to inform the Member State on whose territory the target is or has been intercepted about the interception concerned.

The EU Member States also concluded an additional protocol to the new EU Convention of 2000. The 2001 Protocol[58] aims at further improving mutual assistance within the EU, for instance, by restricting the effect between Member States of reservations and restrictive declarations[59] concerning the execution of letters rogatory aimed at carrying out search/seizure orders. Moreover, refusal of mutual assistance on the basis of either banking secrecy or commercial confidentiality rules is explicitly excluded. In addition, specific provisions have been introduced

[56] European Convention on Mutual Assistance in Criminal Matters, ETS No. 30, Strasbourg, 20.IV.1959.

[57] Criminal investigation is described as follows: "an investigation following the commission of a specific criminal offence, including attempts in so far as they are criminalized under national law, in order to identify and arrest, charge, prosecute or deliver judgement on those responsible". See art. 20(1) 2000 Convention.

[58] Council Act of 16 October 2001 establishing, in accordance with Article 34 of the Treaty on European Union, the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, [2001] OJ C 326/1.

[59] Provided by, for instance, art. 5 of the 1959 Council of Europe Convention.

to facilitate the transfer of information on bank accounts and banking operations. Most revolutionary is the introduction of a possibility to have recourse to so-called discrete account monitoring or "bank account tapping". The fiscal exception was completely banned, and in as far as serious forms of organized crime or money laundering are concerned, assistance can no longer be refused except in case where granting assistance is likely to negatively impact on the fundamental interests of the requested state (*ordre public*).

Apart from the introduction of substantially interesting and important novelties, a number of critiques remain. Most importantly, the approach taken towards mutual assistance is primarily law enforcement oriented. The focus has deliberately and rather exclusively been on accelerating, simplifying and reinforcing mutual legal assistance.

Firstly, there has been great reluctance to introduce data protection safeguards in the Convention. It is yet the first time that a convention on judicial cooperation in criminal matters has incorporated rules on protecting personal data exchanged between two or more Member States (Article 23). The expression "personal data"[60] refers to any information relating to an identified or identifiable individual ("data subject") and it applies irrespective of the way in which the personal data concerned are filed or processed (i.e. automatically or not).[61]

Secondly, in the context of interception of telecommunications, there was hesitation to give the Member State where the target is located or where the target has moved to the right to check whether the intended/continued interception would be/is allowed according to the fundamental principles of its domestic law. Thirdly, there is a striking presumption of compliance with the standards of the ECHR. Finally, no humanitarian or fundamental rights-oriented grounds for refusal (*e.g.* non-discrimination, *ne bis in idem*) have been introduced.

There is in fact an attempt to promote the – almost blind – mutual recognition of any type of judicial decision in criminal matters, including in the context of mutual assistance in criminal matters. The Commission has on multiple occasions[62] announced that the entire mutual assistance *acquis* (including the 2000 Convention and its 2001 Protocol), will be replaced in the years to come with mutual recognition schemes, building on politically presumed full mutual trust between Member States.

Between the EU and third countries

[60] The expression is used within the meaning of the definition of that expression in Article 2(a) of the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[61] See Explanatory report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union, [2000] *OJ* C 379/7.

[62] *e.g.* in the explanatory memorandum to the proposed Framework Decision on the European Evidence Warrant. See Proposal for a Council Framework Decision on the European Evidence Warrant for obtaining objects, documents and data for use in proceedings in criminal matters, COM(2003) 688 final, Brussels, 14.11.2003, pp. 4-5.

Cross-border cooperation in criminal law matters between the EU and third countries has taken the shape of MLA agreements.[63] In transatlantic relations, this has been the case most notably in relation to the EU-US Agreement on MLA (EU-US MLA). This agreement constitutes a flexible tool for cooperation, which provides a broad basis for exchange of information as well as a number of exceptions allowing for a wide array of judicial assistance options. The EU-US MLA contains a rather weak data protection framework, and privacy concerns rarely constitute a barrier to cooperation. The EU-US agreement must be interpreted in light of EU Treaties, the EU Charter as well as European secondary legislation.

A key provision of the EU-US MLA is Article 4, which allows for the exchange of a wide range of everyday information about financial transactions.
Another important provision is Article 8. It aims at extending the scope of the agreement by allowing mutual legal assistance to administrative authorities, investigating conduct with a view to a criminal prosecution of the conduct, or referral of the conduct to criminal investigation or prosecution authorities, pursuant to its specific administrative or regulatory authority to undertake such investigation. The scope of assistance is thus very broad. It seems inconsistent with the tight demarcation of authorities allowed to operate mutual recognition in criminal matters under EU law.

In an effort to address concerns with regard to the adverse impact that its provisions may have on EU privacy and data protection standards, the EU-US MLA contains a specific provision, Article 9 ("Limitations on use to protect personal and other data"). Yet, the wording of this article has done little to address these concerns. The purpose of MLA is so wide that it is questionable whether it meets the fundamental EU data protection principle of purpose limitation.

Art. 9(2) further weakens the already limited data protection framework. While its first part (Article 9(2)(a)) allows States to impose additional conditions in order to comply with a request, its second part (Article 9(2)(b)) states that generic restrictions with respect to the legal standards of the requesting State for processing personal data may not be imposed by the requested State as a condition under subparagraph (a) to providing evidence or information. This is an attempt to ensure that concerns with regard to EU data protection law will not constitute a barrier to cooperation under the MLA Agreement.

By virtue of the non-derogation clause under Article 13, the requested State may invoke grounds for refusal of assistance available pursuant to a bilateral mutual legal assistance treaty, or, in the absence of a treaty, its applicable legal principles, including where execution of the request would prejudice its sovereignty, security, *ordre public* or other essential interests. Non-

[63] See Carrera, S. et al. (2015), *Access to Electronic Data*, pp. 44.47.

compliance with fundamental rights might constitute such a ground for refusal, especially after the entry into force of the Treaty of Lisbon. The Agreement should be interpreted consistently with the requirements of EU constitutional and human rights law, including in particular the provisions laid out above in the scope of the EU Charter as well as consistently with the Directive on the European Investigation Order.

3.2.2. The European Investigation Order

In 2014, after more than a decade of efforts in negotiating it, a major step forward in the international cooperation in evidence gathering among EU Member States was the adoption of the European Investigation Order (EIO).[64] The EIO becomes the sole legal instrument regulating the exchange of evidence and mutual legal assistance between EU Member States. It thus helps in overcoming the undesirable fragmentation of legal instruments for the collection and transfer of evidence between EU Member States,[65] in compliance with the defendants' fundamental rights.[66]

The EIO Directive encompasses two main parts: Chapters I-III introduce the rules underpinning the application of the principle of mutual recognition in the exchange of evidence; Chapters IV-VI consist of specific procedural provisions covering the conduct of investigations (*e.g.* temporary transfer of evidence, hearing by videoconference, covert investigations and the interception of telecommunications and - most notably for the purpose of this Report - access to electronic data).

An EIO is a judicial decision to obtain evidence which has been issued or validated by a judicial authority of a Member State (the issuing State) to have one or several specific investigative measures carried out in another Member State (the executing State). It may also be issued for obtaining evidence that is already in possession of the competent authorities of the executing State (art 1(1)). Most interestingly, its issuing may also be requested by a suspected or accused person (or by his/her lawyer) (art. 1(3))[67].

[64] Directive 2014/41/EU regarding the European Investigation Order in criminal matters, [2014] OJ L130/1.

[65] The Directive replaced, as of 22 May 2017 (transposition deadline for Member States), the corresponding provisions applicable between Member States bound by it the 1959 Council of Europe Mutual Legal Assistance Convention (ETS 30) and its 1978 and 2001 Protocols (ETS 99 and ETS 182); the 2000 Convention implementing the Schengen Agreement and the EU 2000 Mutual Legal Assistance Convention and its 2001 Protocol; the Framework Decision on the European Evidence Warrant (2008/978/JHA), and the relevant provisions of the Framework Decision on the mutual recognition of freezing orders (2003/577/JHA).

[66] Ruggeri, S. (2014), "Introduction to the Proposal of a European Investigation Oder: Due Process Concerns and Open Issues" in Ruggeri, S. (ed.), *Transnational Evidence and Multicultural Inquiries in Europe,* Springer, pp. 29–35; See Carrera, S. et al., *Access to Electronic Data*, pp. 48-54.

[67] By virtue of article 4, it may be issued: (a) With respect to criminal proceedings that are brought by, or that may be brought before, a judicial authority in respect of a criminal offence under the national law of the issuing State; (b) In proceedings brought by administrative authorities in respect of acts which are punishable under the national law

The Directive states expressly that Member States must execute the EIO on the basis of the principle of mutual recognition (art. 1(2)). In principle, the executing authority must recognise an EIO without any further formality being required, and ensure its execution, in the same way and under the same modalities as if the investigative measure concerned had been ordered by an authority of the executing State (art. 9(1)). The decision on the recognition or execution must be taken and the investigative measure must be carried out with the same celerity and priority as for a similar domestic case and, in any case, within the time limits provided in the Directive (art. 12(1)).

The Directive thus introduces a system of mutual recognition based on speed, and a minimum of formality. It provides, however, for a number of safeguards which temper the automaticity in the execution of EIOs. These provisions concern in particular: the possibility of legal adaptation in the execution of an EIO; the introduction of a proportionality test; and the introduction of a specific ground for refusal to execute on fundamental rights grounds.

Firstly, the Directive provides a series of safeguards for the respect of the legal and constitutional system of the executing Member State.[68] The Directive requires the applicability of legal remedies equivalent to those applicable in a similar domestic case to the investigative measures indicated in the EIO (art. 14(1)). In addition, the Directive has included a key safeguard as regards the integrity of the law of the issuing State. The Directive states clearly that the issuing authority may only issue an EIO where the investigative measures indicated therein could have been ordered under the same conditions in a similar domestic case (art. 6(1)(b))[69].

---

of the issuing State by virtue of being infringements of the rules of law and where the decision may give rise to proceedings before a court having jurisdiction, in particular in criminal matters; (c) In proceedings brought by judicial authorities in respect of acts which are punishable under the national law of the issuing State by virtue of being infringements of the rules of law, and, where the decision may give rise to proceedings before a court having jurisdiction, in particular, in criminal matters; and (d) In connection with proceedings referred to in points (a), (b) and (c) which relate to offences or infringements for which a legal person may be held liable or punished in the issuing State.

[68] *e.g.* the executing authority must comply with the formalities and procedures expressly indicated by the issuing authority provided that these are not contrary to the fundamental principles of law of the executing State (art. 9(2)); may also have recourse to an investigative measure other than that indicated in the EIO where the investigative measure selected by the executing authority would achieve the same result by less intrusive means (art. 10(3)).

[69] This prevents Member States from obtaining evidence abroad which they are not able to obtain under their own domestic legal and constitutional procedures.

Secondly, the EIO Directive introduces a proportionality test,[70] which is reserved for the issuing authority: an EIO must be necessary and proportionate (art. 6(1)(a)). This is meant to prevent abuses.[71]

Thirdly, the EIO Directive contains a general clause proclaiming respect for fundamental rights, as well as, for the first time, an express ground for refusal on fundamental rights grounds. The executing authority may refuse to recognise or execute an EIO where there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter (art. 11(1)(f)). The executing authority must thus examine the impact of the execution of the EIO on the affected individual. States should also endeavour to establish fluent consultation channels with the authorities of the other Member States involved in the execution of EIOs.

This major legal development expressly establishes the fundamental rights parameters of the operation of the mutual recognition principle.[72] The provision sets limits to blind mutual trust among Member States and confirms that the presumption that all Member States comply with fundamental rights at all instances is rebuttable.[73]

As we have seen in this section, the EIO regulates the exchange of evidence between EU Member States in the area of criminal justice. The path towards the adoption of this instrument was lengthy and difficult. The challenge was that of allowing for the swift and efficient cross-border judicial cooperation in criminal investigations in the EU and the admissibility of the evidence obtained abroad, while ensuring a high standard of procedural rights of the defendants involved in them. One of the particularities of the EIO is that it is based on principle of mutual recognition and mutual recognition is the objective to be achieved, but it takes into account the

[70] In the context of the implementation of the Framework Decision 2002/584/JHA on the European Arrest Warrant a debate has arisen as to whether the operation of mutual recognition in criminal matters should be subject to a proportionality test. And, if so, whether this test should be conducted by the issuing or by the executing authority, or by both. In fact, national law enforcement authorities had been allegedly issues EAWs with reference to minor offences. The criminal justice system was thus inundated by large numbers of requests resulting in high costs and delays, which have adverse effects on both the efficiency of the system and the fundamental rights of the concerned individuals.

[71] Allegrezza, S. (2014), "Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality", in Ruggeri, F. (ed.), *Transnational Evidence and Multicultural Inquiries in Europe,* Springer, p. 51–67.

[72] Over the years, the inclusion of an express ground of refusal to recognise and execute a judicial decision on fundamental rights grounds have been a central question in the development of the application of the principle of mutual recognition in criminal matters. Before the entry into force of the Lisbon Treaty, EU mutual recognition instruments in the Third Pillar contained references to the respect of fundamental rights but did not include a specific ground for refusal in this regard.

[73] Armada, I. (2015), "The European Investigation Order and the Lack of European Standards for the Gathering of Evidence. Is a Fundamental Rights-Based Refusal the Solution?" 1 *New Journal of European Criminal Law,* p.8.

flexibility of the traditional mutual legal assistance mechanisms.[74] This approach was criticised by those who desired a strict application of the mutual recognition principle and claimed that within the EU AFSJ, the requested Member States should barely have any possibility to refuse requests for evidentiary assistance coming from other Member States. At the same time, the EIO was also criticised for trying to go too far too early in building up a single European judicial area: some Member States were not willing to apply in their territories investigative measures that were assessed as disproportionate or against their own laws and constitutional principles, just to comply with the principle of mutual recognition.[75]
Special efforts must be devoted to consolidating or creating mutual trust, but also for showing understanding towards different legal and constitutional traditions.

The implementation of the EIO will definitely facilitate the cooperation between Member States in prosecuting crimes. However, the imbalance between the powers of the prosecution and the defendant is at times manifest. In many Member States, the defence is not allowed to gather evidence independently, and can only request the investigating authority or court to adopt measures. This is in contrast with the principle of equality of arms. Ultimately, although Article 1(3) EIO directive foresees the possibility for the defendant to have access to cross-border evidence, this will rarely be possible in practice.

Further discussions should be held in order to find some compensation to the defence for the shortcomings detected in relation to this principle. Nevertheless, the Directive does not safeguard the rights of third parties that may be affected when executing an EIO, save for the rules on witnesses' and experts' testimonies through videoconference, telephone or other audio-visual means (arts. 24 and 25 EIO Directive). Member States' legislation should ensure that third parties are properly informed of measure that affect them and how to protect their rights. This should be done in the executing state by the competent judicial authority; however, it is unclear who should be responsible for informing when a measure (*e.g.* the interception of communications) has been executed directly by and from a foreign state without the technical assistance of the Member State in which the third person is located.

3.3. Main questions dealt with by landmark rulings

This section examines the role of European courts in operating the balancing exercise between the rights to privacy and the protection of personal data on the one hand, and conflicting interests and rights on the other hand.

[74] Bachmaier, L. (2017), "Mutual recognition and cross-border interception of communications: the way ahead of the European Investigation Order" in Brière, C. and A. Weyembergh (eds.) *The needles balances in EU criminal law: past, present and future*, Oxford: Hart.
[75] Zimmermann, F. et al (2011), "Mutual Recognition and its Implications for the Gathering of Evidence in Criminal proceedings: a Critical Analysis of the Initiative for a European Investigation Order", *European Criminal Law Review,* 1, p. 56.

This is because the way in which EU legislation was drafted was at that time vague and left a margin of interpretation to both the national legislator during the transposition process and also to a certain extent when provisions are applied in practice. The CJEU thus intervened at times to ensure even and consistent interpretation and application of EU law throughout the continent and consequently safeguard EU citizens' rights; the ECtHR has also welcomed individual challenges to redress situations where the right to privacy had been breached and national remedies had been exhausted.

3.3.1. The Court of Justice of the European Union

The Court of Justice of the European Union (CJEU) has decided several cases with far-reaching implications for the rights to privacy and the protection of personal data in the European Union, the most notable of these being the rulings in *Google Spain*, *Digital Rights Ireland,* and *Schrems, Tele2/Sverige*.[76]

In *Google Spain* the CJEU held that the 1995 DPD requires search engine operators to remove links to web pages which are shown when a person is searched for by name. In this way a broad scope of application of the DPD was maintained: this was done by considering a search engine operator as a 'data controller' within the meaning of Article 2(d) of the DPD and its activities as being classified as the 'processing of personal data' for the purposes of Article 2(b) of the DPD.

A high level of attention for data protection has also been shown by the CJEU through the invalidation of the 2006 Data Retention Directive in *Digital Rights Ireland*. In this case the CJEU acknowledged that while data retention is necessary for the investigation, detection and prosecution of serious crimes, the EU legislature had exceeded the limits imposed by the proportionality principle (Article 52(1) EU Charter) because of the extent and seriousness of interference of provisions on fundamental rights to privacy (Article 7 EU Charter) and protection of personal data (Article 8 EU Charter),[77] interferences which are not limited to what is strictly necessary.[78] This is the case because the Directive:

(1) concerns all individuals, all means of electronic communication and all traffic data without differentiation, limitation or exception made in the light of the objective of fighting serious crime;[79]
(2) fails to identify substantive or procedural conditions ensuring that competent authorities

[76] *Google Spain and Google*, Case C-131/12, 13 May 2014; *Digital Rights Ireland* and *Seitlinger and Others*, Joined Cases C-293/12 and C-594/12, 8 April 2014; *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14, 6 October 2015; Tele2 Sverige AB, C-203/15, 21 December 2016.
[77] *Digital Rights Ireland and Seitlinger and Others*, para. 26-27 and 35-37.
[78] Ibid., para. 65.
[79] Ibid., para. 58-59.

have access to the data and use them only for the purposes of prevention,[80] investigation, detection and prosecution of serious crime;[81]
(3) establishes no distinction between categories of data or its usefulness in relation to the objective pursued, thus modulating data retention periods accordingly;[82]
(4) encompasses no objective criteria to determine retention periods and thus ensure that it is limited to what is strictly necessary;[83]
(5) provides insufficient safeguards against the risk of abuse, particularly with reference to unlawful access and use of data.[84]

Digital Rights Ireland provides *a contrario* a set of instructions to devise a new data retention framework. From the ruling it emerges first and foremost that bulk data retention (meaning indiscriminate retention of personal data of unsuspicious individuals) is an option to be excluded in a future data retention instrument. In the CJEU's opinion this is because of its disproportionate impact on the data privacy rights. Secondly, retention periods must be determined according to data's potential usefulness and should remain as short as possible. Thirdly, during retention periods effective mechanisms should ensure a very high level of protection and security, under the oversight of an independent authority.

Fourthly, access and use of data by law enforcement authorities when it has been retained by Internet Service Providers (ISPs) for commercial purposes should be restricted to what is 'strictly necessary', and must respect the following procedural and substantive conditions: access and use by competent national authorities should be limited to the purpose of investigating, detecting and prosecuting precisely defined serious offences.[85] Requests for access to retained data should be reasoned and subject to prior review by a court or an independent administrative authority charged with ensuring compliance with constitutional and legislative limits to data access and use. Specific legislative safeguards should provide access to and use of data to a limited number of agencies or law enforcement authorities as well as a limited number of individuals inside the requesting institutions.[86]

The transatlantic aspect of data protection was brought to the attention of the CJEU in *Schrems*.[87] The CJEU invalidated the Commission's decision to put into effect the Safe Harbour

[80] It is worth highlighting that prevention purposes appear only in the Preamble of the Directive and not in the body of the text, which refers only in its Article 1 (Subject matter and scope) to the investigation, detection and prosecution of serious crime. However, the CJEU does not make such distinction in the judgment.
[81] *Digital Rights Ireland*, para. 60-62.
[82] Ibid., para. 63.
[83] Ibid., para. 64.
[84] Ibid., para. 66-68.
[85] Granger, M.-P. and K. Irion (2014), *European Law Review,* Vo. 39, No.6, p. 836.
[86] *Digital Rights Ireland and Seitlinger and Others*, para. 61-62.
[87] Mr Schrems complained to the Irish data protection authority (DPA) about the transfer of his personal data pursuant to Safe Harbour provisions, as a Facebook user. However, the DPA refused to consider the complaint

agreement[88] and considered data transfers to the USA as not receiving an 'adequate level of protection'.[89]

The CJEU elaborates upon the validity of the Safe Harbour decision in the context of an overall analysis of the architecture of EU data protection law. Firstly, as it does not clearly emerge in the Directive what an 'adequate level of protection' is, the CJEU interprets it as a 'high level' of protection in the third country, which does not need to be 'identical' to EU standards but must be 'essentially equivalent' to it. Means used in the third state to ensure data protection rights must be 'effective', although they 'may differ' from that in the EU. [90] The adequacy assessment must also be dynamic, with regular automatic reviews and an obligation for a further review if 'doubts' emerge; general changes in circumstances since the adoption of a decision must be taken into account.[91] Secondly, in light of the significance of data privacy rights and the number of people affected by an inadequate level of protection in a third country, the CJEU considers the Commission has reduced discretion, and is subject to 'strict' standards of judicial review.[92]

Thus, the Safe Harbour decision considering adequate data protection standards in the US was declared invalid. According to the Court, the Commission should base Adequacy Decisions on the level of protection afforded by domestic legislation or the international commitments of the third country in question. As such, in the CJEU's view, the self-certification system adopted in the challenged Adequacy Decision[93] does not meet this requirement as it only binds US companies

---

because it was bound by the Commission's decision. Mr. Schrems challenged the DPA's decision before the Irish High Court, which doubted the system's compliance with EU law (or indeed the Irish constitution), and thus sent a reference for a preliminary ruling to the CJEU asking whether the DPA was bound by the Commission's Decision, and whether it can conduct its own examination.

[88] The 'Safe Harbour' agreements refer to the seven 'Safe Harbour Privacy Principles': Notice - Individuals must be informed that their data is being collected and about how it will be used. They must provide information about how individuals can contact the organization with any enquiries or complaints; Choice - Individuals must have the option to opt out of the collection and further transfer of the data to third parties; Onward Transfer - Transfers of data to third parties may only be to other organizations that follow adequate data protection principles; Security - Reasonable efforts must be made to prevent loss of collected information; Data Integrity - Data must be relevant and reliable for the purpose it was collected for; Access - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate; Enforcement - There must be effective means of enforcing these rules.

[89] See Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, [2000] OJ L 215/7.

[90] *Schrems*, para. 73-74.

[91] Ibid., para. 76.

[92] Ibid., para. 78.

[93] A self-certification process entails that US companies may self-certify that they would comply with EU data protection standards in order to allow for transfer of personal data from the EU to the US. The CJEU considered in *Schrems* that although the Commission's adequacy decision could be based on self-certification, this has to be accompanied by 'effective detection and supervision mechanisms' ensuring that infringements of fundamental rights would be 'identified and punished in practice' (para. 81).

and not US public authorities.[94]

In addition, the CJEU scrutinized the exceptions contained in the Adequacy Decision that allowed derogations to data protection without any limitation, based on legitimate interests such as national security requirements established by US law. Within the EU, interference with data privacy rights requires 'clear and precise rules' which set out minimum safeguards, as well as strict application of derogations and limitations.[95] Those principles were considered by the CJEU as being breached where, 'on a generalised basis', legislation authorizes 'storage of all the personal data of all the persons whose data has been transferred' to the US 'without any differentiation, limitation or exception being made in light of the objective pursued' and without any objective test limiting access of the public authorities for specific purposes.[96] The CJEU expressly reasserted the limits to mass surveillance established in *Digital Rights Ireland*: general access to the content of communications compromises the 'essence' of the right to privacy[97] and thus constitutes an unjustifiable violation of the Charter (Articles 7 and 8).

The *Schrems* case reasserts requirements that have been in place since *Digital Rights Ireland*: a new data retention instrument should provide sufficient safeguards to limit the storage of personal data of targeted unsuspicious individuals; public authorities' access to retained data should be based on objective criteria and further use of such data should be restricted, the content of electronic communications being accessible under limited circumstances only. Finally, individuals should be granted the possibility to pursue legal remedies to access their personal data, or to obtain the correction or erasure of such data.[98]

On 21 December 2016 the CJEU delivered its judgment in *Tele2 Sverige AB and Watson*. The Court had been asked by a Swedish and British court respectively to consider the scope and effect of its previous judgment in *Digital Rights Ireland*. The judgment, about the E-Privacy Directive, reflects continuity in so far as it follows in the line of this, and earlier judgments taking a strong stance on data protection and privacy.

The CJEU states that data retention must be restricted to (i) particular time periods and/or geographical and/or a group of persons likely to be involved, in one way or another, in a serious crime or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime.[99] The Court outlines a targeted data retention regime which does not include every subscriber.[100] In the second part of the judgement, the CJEU sets out strict access

[94] *Schrems*, para. 82.
[95] Ibid., para. 91-92.
[96] Ibid., para. 93.
[97] Ibid., para. 94.
[98] *Schrems*, para. 91-93.
[99] *Tele2 Sverige AB*, para. 106.
[100] Ibid., para. 108-111.

conditions. Access to retained data must be solely for the purpose of fighting terrorism and serious crime and must be subject to a prior court review. With the exception of terrorism cases, access can only be granted to data of individuals suspected of involvement in serious crime.[101]

The degree of protection the judgement offers to the rights of privacy and data protection over competing interests, notably security, is radical. In particular, the Court unequivocally states that legislation providing for general and indiscriminate data retention is incompatible with the E-Privacy Directive, as read in light of the relevant EU Charter rights, *i.e.* Articles 7, 8 and 52(1). One could argue that the Tele2 judgment is even stricter than the CJEU invalidation of the Data Retention Directive in *Digital Rights Ireland* as Article 15(1) of the e-Privacy Directive makes data retention an exception to the main rule of erasure once the communication is completed.

Moreover, while the judgment was delivered in the context of the E-Privacy Directive, the Court's reasoning could equally apply to other EU secondary legislation or programs interpreted in light of the Charter. This judgment has received a very mixed reaction from EU Member States as such. While national data retention legislation has been annulled across multiple Member States, this annulment has been based on an assessment of the proportionality of the relevant measures rather than on a finding that blanket retention is *per se* unlawful. The *Tele2* judgment thus represents a rupture with the past in one very significant way: the CJEU, for the first time, unequivocally states that blanket data retention measures are incompatible with EU law, read in light of the Charter.

Secondary law on privacy and data protection (before the Data Protection Package reform) has been interpreted by the CJEU on several occasions.[102] Yet recent case law reflects heightened attention towards safeguarding the right to data protection.

These four rulings exemplify the need to strike a delicate balance between the right to data protection and several conflicting rights and values. It is for the EU legislator and the courts to strike this balance. The CJEU case law has set a number of strict requirements for the EU legislator to comply with when devising any provision which may clash with the rights to privacy and protection of personal data. The four cases have insisted on the centrality and almost sacred value of the two rights. Of course, neither privacy or data protection are absolute rights which cannot be limited. Yet the CJEU requires strict justification of limitations, transparency and procedural safeguards. In particular, in these cases, the Luxembourg Court uses a strict necessity

[101] Ibid., para 119.

[102] See for instance, *Lindqvist*, Case C-101/01, 6 November 2003; *Rechnungshof v. Österreichischer Rundfunk*, Joined Cases C-465/00 and C-138/01, 20 May 2003; *Parliament v. Council*, Joined Cases C-317 and C-318/04, 30 May 2006; *Promusicae*, Case C-275/06, 29 January 2008; *Ireland v. Parliament and Council*, Case C-301/06, 10 February 2009; *Huber v. Germany*, Case C-524/06, 16 December 2008; *Satamedia*, Case C-73/07, 16 December 2008; *Schecke and Eifert,* Joined Cases C-92/09 and C-9309, 9 November 2010; *Probst*, C-119/12, 22 November 2012; *Bara and Others*, Case C‑201/14, 1 October 2015; *Weltimmo*, Case C‑230/14, 1 October 2015.

and proportionality test. Does the CJEU imply that the rights to the protection of personal data are super-rights that should take absolute precedence over others?[103] An affirmative answer would be in stark contrast with CJEU precedent that data protection must be considered in relation to its function in society[104] and that EU data protection law has territorial limits and is not to be seen as a system of universal application.[105]

In a sort of inter-institutional dialogue, the main message of these CJEU cases is not that the rights to privacy and the protection of personal data transcend any form of balancing, but rather that it is for the EU legislator to take the lead to ensure that, notwithstanding the fact they are both enshrined in the Charter, the rights to privacy and the protection of personal data are not neglected when drafting EU legislation. Most importantly the CJEU calls for the EU legislator to define key concepts, procedures to follow for the protection of processed data and authorities who may access and make use of such data more clearly.

From *Digital Rights Ireland* it emerges first and foremost that bulk data retention is an option to be excluded in a future data retention instrument. In Schrems, the CJEU expressly reasserted the limits to mass surveillance established in *Digital Rights Ireland*: general access to the content of communications compromises the 'essence' of the right to privacy and thus constitutes an unjustifiable violation of the Charter (Articles 7 and 8). In *Tele2* the CJEU, for the first time, unequivocally states that blanket data retention measures are incompatible with EU law, read in light of the Charter.

All cases clearly state that arbitrary retention of data of unsuspicious individuals is not acceptable. CJUE case law is not only relevant in the context of specific cases but more broadly, for the regulation of data retention and sharing within the EU and with third-country. This emerges clearly in the latest Commission proposals on e-evidence, whereby the safeguard of privacy requires the introduction of procedures to hinder any automatic transmission of e-evidence without due consideration of data protection.

3.3.2. The European Court of Human Rights

Article 8 ECHR explicitly establishes a right to respect for private life, as well as a right to family life, the inviolability of the home and the confidentiality of communications. The European Court of Human Rights (ECtHR) has interpreted and thus detailed the scope of the article and the necessary requirements for interference to be regarded as lawful and legitimate.

[103] Kuner, C. (2014), "A "Super-right' to data protection? The Irish Facebook Case and the future of the EU data transfer regulation", *Concurring Opinions (Blog)* (http://concurringopinions.com/archives/2014/06/the-data-retention-judgment-the-irish-facebook-case-and-the-future-of-eu-data-transfer-regulation.html).
[104] *Schecke and Eifert*, para. 48.
[105] *Lindqvist*, para. 69 and 90.

In *Malone v. the United Kingdom*,[106] the Strasbourg Court made clear that the existing rules and practices in the United Kingdom did not satisfy the requirement of art. 8 ECHR that any interference with a person's privacy by a public authority should be 'in accordance with the law'. In fact, the disclosure of 'metadata' to law enforcement thus constitutes a breach of Article 8 of the ECHR in absence of clear rules delimiting the role of public authorities.

In *Taylor-Sabori v. the United Kingdom*,[107] the applicant's communications had been accessed through a 'clone' of the applicant's pager, and he was subsequently arrested and charged with conspiracy to supply a controlled drug. As at the time there was no provision in British law allowing for such interception, the interference was regarded by the ECtHR as not being "in accordance with law". The Strasbourg Court stressed that such a requirement demands the existence of a provision of domestic law that must have certain qualities.
In *Liberty and others v. the United Kingdom*[108], the ECtHR decided that any State interference over human rights provisions in a law enforcement context needs to be firmly anchored in legislation meeting the following three standards: first, the practice needs to have its basis in national law; second, the law must be accessible and sufficiently clear and precise to the individual; third, the consequences need to be foreseeable (foreseeability).

The ECtHR has interpreted the scope of Article 8 ECHR as encompassing the compilation of data about individuals by public authorities.[109] The Court has held in different judgments that the right to private life can be infringed by the collection, registration or use of personal information.[110] The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8, and that the subsequent use of the stored information has no bearing on that finding. In determining whether the personal information retained by the authorities involves any relevant private-life aspects, the Court will have due regard to the specific context in which the information has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.

The Strasbourg Court has declared in *Marper v. the United Kingdom* that the protection of personal data is "of fundamental importance" for the enjoyment of the right to respect for private life guaranteed by Article 8 ECHR. Domestic laws must afford appropriate safeguards to prevent any use of personal data that may be inconsistent with its guarantees.[111] The Court has

[106] ECtHR, Malone v. United Kingdom, Judgement of 2 August 1984, Application No 8691/79.
[107] ECtHR, *Taylor-Sabori v. the United Kingdom,* Judgement of 22 October 2002, Application No. no. 47114/99.
[108] *Liberty and others v. the United Kingdom*, Judgement of 22 June 2002, Application no. 58243/00.
[109] *Uzun v Germany*, Judgement of 2 September 2010, Application. No. 35623/05.
[110] See Brouwer, E. (2008), *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Martinus Nijhoff Publishers.
[111] *S. and Marper v. The United Kingdom*, Judgement of 4 December 2008, Applications nos. 30562 /04 and 30566/04.

also emphasised that the need for such safeguards "is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes". It has examined multiple situations related to the storage of personal data by public authorities.[112]

First, according to *Marper*, the retention of samples should only be allowed for the most serious offences and not just for any recordable offence. Indefinite retention should not be possible, and a maximum limit should be established either via primary or secondary legislation.

Secondly, it should be specified whether samples and DNA profiles would be deleted after the acquittal of an individual. Thirdly, detailed rules should exist as to who can access the database and under which circumstances. Fourthly, as proposed by the House of Lords during the discussion of the Counter-Terrorism Bill 2008, it should be possible for an individual to request a statement of what information is held on him in the database. Finally, an individual should be able to request the destruction of information or samples retained under certain circumstances.
The Strasbourg Court has also specifically acknowledged the importance of avoiding the use of incorrect personal data in police reporting in criminal proceedings. In *Cemalettin Canli v. Turkey*,[113] the Court found a violation of Article 8 of the ECHR following the unsuccessful requests made by the applicant to have amended an inaccurate police report submitted to a court in criminal proceedings, as well as police records. The ECtHR explicitly asserted that the information in the police report was within the scope of Article 8 of the ECHR.[114]

In *Zakharov v. Russia*, the ECtHR has begun to address the question of mass surveillance and whether the indiscriminate acquisition of vast amounts of data should not be permissible.[115] In particular, similarly to the case-law developments in Luxembourg, the Strasbourg Court has recently reasserted that in the name of the right to privacy, clear limits must be identified to public authorities' surveillance of unsuspicious individuals. "Private life", asserted the Court, is a broad term not susceptible to exhaustive definition, and that the protection granted under Article 8 of the ECHR is not limited to the private sphere or the home of the individual.

In **Szabó v. Hungary**[116] the ECtHR declared that Hungarian surveillance law contravenes the right to privacy enshrined in the European Convention on Human Rights. In doing so, the Court reinforced the findings of the Grand Chamber in *Zakharov v. Russia* and argued at length on the need for human rights law principles to be "enhanced" to take into account States'

[112] Ibid.
[113] *Cemalettin Canli v. Turkey*, Judgement of 18 November 2008, Application no. 22427/04.
[114] Ibid., para. 33.
[115] ECtHR, *Zakharov v. Russia*, Judgement of 4 December 2015, Application No. 47143/06; ECtHR, *SzaboVissy v. Hungary*, Judgment of 16 January 2016, Application No. 37138/14.
[116] ECtHR, *Szabó and Vissy v. Hungary*, Judgement of 12 January 2016, Application No. 37138/14.

increased appetite for "massive monitoring of communications." The judgment scores the likelihood that the Strasbourg Court intends to definitively outlaw mass surveillance.

Both the Luxembourg and Strasbourg courts have put forward a broader notion of surveillance, in order to address, most importantly within the EU and US but also at a global scale, a generalised, massive pre-emptive surveillance which would have an impact on the individual as a whole. Such judicial action together with political pressure by various stakeholders has put pressure on the legislators to rethink a number of instruments and minimum standards in a different light.[117]

[117] Mitsilegas, V. (2015), "The Transformation of Privacy in an era of pre-emptive Surveillance", *Tilburg Law Review,* Vo. 20, p. 35.

4. Current developments

A number of ongoing developments both in policy making and case-law are worth mentioning as they are likely to influence the issues addressed in this paper.

4.1. More on the Data Protection Package

It is currently unclear how EU and national law will ensure consistency between fundamental rights and effective data retention and sharing. The data protection reform was not designed at all to grasp the reality and highly specific challenges of foreign law enforcement authorities unmediated access practices.

While the GDPR entered into force on 24 May 2016, it only applies as of 25 May 2018. The Police Data Protection Directive entered into force on 5 May 2016 and EU Member States had to transpose it into their national law by 6 May 2018. Public lights were mostly cast upon the GDPR; yet the Directive requires some additional attention now at the final stage of implementation in order to properly asses its contribution to data protection purposes. While one could argue that the actual final provisions of the Directive could have been better in many ways, the EU now has a data protection instrument that sets the threshold for compromise between effective law enforcement authorities' activities and the individual right to data protection. Member States must, however, address a number of shortcomings while incorporating the Directive into their national law. Most importantly, the Directive leaves out of its scope technology-led policing such as the application of data analytics to the work of law enforcement authorities, including profiling. By contrast, one would have hoped for the introduction of special, customised, more effective data protection safeguards in this realm to avoid a generalised intelligence personal data processing to be undertaken by every law enforcement agency.

Moreover, the data protection reform package remains incomplete. In particular, a regulation is currently under negotiation which will replace the E-Privacy Directive, and clarify and supplement the GDPR, with regard to personal electronic communications data.[118] The Commission proposal clarified that communications between machines are subject to the same safeguards as communications between humans. Current drafts of the e-privacy Regulation require that processing electronic communications metadata (other than for specified purposes) requires consent. This is more restrictive than the regime under the GDPR, which provides

[118] Proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 10 January 2017.

several alternatives to consent which can be relied upon to process personal data (*e.g.* "purpose compatibility" by virtue of art. 6 GDPR).

This negotiation has most importantly provided a forum for discussions on the issue of data retention, as it opens up the possibility of including data retention provisions in the forthcoming Regulation.[119] On 15 September 2017, the EU Counter-Terrorism Coordinator (EU CTC) submitted a new data retention proposal to Member States.[120] Considering input received from Member States, he makes it clear that he is not at all interested in targeted data retention. Instead, the EU CTC proposes the concept of "restricted data retention" (instead of "targeted data retention") on the basis that it is necessary to fight terrorism and serious crime. This measure has to be limited to the strictly necessary and be based on objective evidence. However, the measure could cover the entire population, even though this is quite obviously blanket data retention. The EU CTC suggests that the draft E-Privacy Regulation could be amended to make blanket data retention easier. In his view, the EU legislator should, allow storage of communications data in Article 7 of the draft E-Privacy Regulation if legally required to assist governments to fight serious crime and terrorism. However, a provision of this type would still be a restriction on the fundamental rights to privacy and data protection of subscribers, and the restriction would have to satisfy the conditions of Article 52(1) of the Charter of Fundamental Rights. This would not necessarily be different from the current situation with Article 15(1) of the E-Privacy Directive or Article 11 of the draft e-Privacy Regulation.

4.2. A new data retention directive?

Notwithstanding the possibility of having specific provisions in the e-Privacy directive, an EU instrument that harmonizes **data retention** regimes and thus indirectly ensures comparable data protection standards within the region would be the most appropriate solution. The best legal instrument for this would be a directive because as it better accommodates differences existing between the criminal law systems of Member States. A criminal law legal basis for it would allow the EU legislature to avoid vague terminology and not hinder an effective tackling of serious cross-border criminal activity and an equal and consistent safeguarding of data privacy rights throughout the continent.

And how is the EU responding to this issue through policy measures? Several EU governments urged the EU to present a legislative initiative for a new Data Retention Directive. But in 2015, it

[119] See for instance the position of a wide number of EU Member States, and Europol, on the possibility of including mandatory data retention rules in the ePrivacy Regulation. General Secretariat of the Council Working document, Contributions by delegations, WK 9374/2017 REV 1, LIMITE, 15 September 2017.

[120] EU Counter-Terrorism Coordinator, Working document on contributions to the discussion on data retention, WK 9699/2017 INIT, LIMITE, 15 September 2017. See also Retention of communication data for the purpose of prevention and prosecution of crime, Council document 13845/17, LIMITE, 30 October 2017.

was announced that there will be no legislative initiative on this matter.[121] In the European Agenda on Security, the Commission reaffirms the value of communication data for the purpose of an effective prevention and prosecution of terrorism and organized crime. There is no mention of a possible legislative initiative; the Commission simply commits itself to continue monitoring legislative developments at national level[122] and the situation has been on hold for the last three years. Notwithstanding the CJEU judgments, the current situation provides for a catalyst to the adoption of national measures, which are not compatible with the CJEU's findings in terms of necessary compliance with the rights to privacy and data protection. Member States consider more data gathering, retention and sharing to be one of the main solutions to cope with terrorism and serious crime. As long as it remains contentious whether more data retention would be a solution *per se,* Member States remain under the current legal framework, in which they set their own data retention rules, thereby possibly hindering effective cooperation in the fight against serious crimes with a cross-border dimension.

4.3. The e-evidence proposals

On 17 April 2018, the Commission presented two new proposals on e-evidence which would enable law enforcement authorities to request ("production request") or compel ("production order") a third party, *i.e.* a service provider, in another Member State, to disclose personal data about a user, without the request or order having to go through a law enforcement or judicial intermediary in the other Member State. The package proposed encompasses a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (on the basis of Article 82(1) TFEU)[123] along with a Directive on the Appointment of Legal Representatives (on the basis of Articles 53 and 62 TFEU).[124] Cooperation will take the form of a European Production Order Certificate (EPOC) or European Preservation Order Certificate (EPOC-PR) directly from an issuing authority in one Member State to the legal representative of service providers in another Member State. Both types of order may only be issued in the context of criminal proceedings either during the pre-trial or trial phase. Compliance by service providers must not depend on the location of the data solicited.[125]

[121] Guarascio, F. (2015), "EU executive plans no new data retention law", *Reuters* (http://www.reuters.com/article/us-eu-data-telecommunications-idUSKBN0M82CO20150312).

[122] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, COM(2015) 185 final.

[123] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 17 April 2018, COM/2018/225 final - 2018/0108 (COD)

[124] Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, 17 April 2018, COM/2018/226 final - 2018/0107 (COD)

[125] This specification reflects the longstanding discussions revolving around the US Microsoft Case. See *infra*.

The draft EPO Regulation is full of references to the EU data protection package. Article 11 provides that the addressee of an EPOC or EPOC-PR must refrain from informing that person,[126] unless the issuing authority requests that this be done. Where the service provider has not already informed the data subject that their data has been subject to an EPOC or EPOC-PR, the issuing authority shall inform the target thereof once there is no longer a risk of jeopardizing the investigation.[127] By virtue of Article 17, once apprised of the situation, the person whose data was obtained via an EPO has the right to effective remedies under the EU data protection *acquis* and under national law before the court in the issuing state. This is the case irrespective of whether the individual is a suspect or accused person or not; hence, whether in criminal or civil proceedings. According to Article 18, immunities and privileges in respect of transactional or content data obtained by virtue of an EPO granted under the law of the Member State of the addressee (the service provider) are to apply in criminal proceedings in the issuing state.

The EPO proposals witness an additional shift away from traditional MLA agreements, involving the "direct" cooperation between law enforcement authorities seeking to obtain electronic evidence and the foreign service providers in (exclusive) control of it. MLA existing mechanisms are in fact considered lengthy and complex. Law enforcement authorities thus often disregard them in order to address requests for information directly to foreign service providers, via a domestic investigative measure, bypassing the judicial authority where service providers are established or targets habitually resident. Such mechanisms constitute a *de facto* extraterritorial reach of national investigative powers, and an extension of the "sword" function of criminal law via the further privatization of security.

4.4. The transatlantic dimension: the Supreme Court case US v Microsoft and the Cloud Act

The most recent proposals within the EU are deeply influenced by what happens across the Atlantic.

In 2013, US law enforcement authorities served Microsoft a search warrant for emails as part of a US drug trafficking investigation. In response, Microsoft handed over data stored on American servers. However, it did not give the government the actual content of the individual's emails, because they were stored at a Microsoft data centre in Dublin, where the subject lived when he signed up for his Outlook account. In July 2016, the Second Circuit Court of Appeals in New York, ruled that a warrant obtained under the Stored Communication Act 1986 does not allow the government to require the production of emails stored by Microsoft overseas because the

[126] In compliance with Article 23 GDPR.
[127] In accordance with Article 13 Police Data Protection Directive.

relevant provision of the statute does not apply "extraterritorially" to reach foreign-stored data.[128]
In *US v Microsoft*, in front of the Supreme Court, the US government has argued that using MLA Agreements to obtain evidence related to serious crimes is cumbersome and too slow especially if multiple jurisdictions are involved. Civil liberties organizations such as the American Civil Liberties Union, the Brennan Center for Justice, and the Electronic Frontier Foundation all filed an amicus brief to the Supreme Court. Several justices said Congress rather than the court should act to define the limits of privacy in the digital age.

Many expected the US Supreme Court to decide whether territorial borders matter when it comes to data. And hoped the case could have broad and worldwide consequences for foreign law enforcement authorities' unmediated access to data held by private companies.
Yet, the decision of the Supreme Court has been partially disappointing.[129]The US government argues that using MLA Agreements to obtain evidence related to serious crimes is cumbersome and too slow, especially if multiple jurisdictions are involved. Civil liberties organizations such as the American Civil Liberties Union, the Brennan Center for Justice, and the Electronic Frontier Foundation all filed an amicus brief to the Supreme Court. In fact, the Court has not decided whether federal prosecutors can force Microsoft to turn over digital data stored outside the United States. The enactment of a new federal law made the case moot. The Court said in a brief, unsigned opinion that "No live dispute remains between the parties".

Microsoft now has a duty to turn over the content of the emails that are hosted on a server in Ireland, given the recent entry into force of the Cloud Act 2018. In fact, the judgment did have a major impact on legislative developments in the US.

In this context, the Cloud Bill, introduced in February 2018 and backed by numerous ICT companies including Microsoft, Apple, Facebook, and Google, addresses many of the questions issues at stake in *US v Microsoft.*[130] It constituted a compromise between the interests of ICT companies and law enforcement authorities.

Until recently, it was unclear whether the government could use the Stored Communications Act 1986 (1986 SCA) to compel US-based network providers to disclose their client communications, records, and information located in a foreign jurisdiction.

[128] See In re Warrant to Search a *Certain Email Account Controlled & Maintained by Microsoft Corp.*, Case No. 14-2985, 2d Circuit, 14 July 2016.
[129] *United States v. Microsoft*, No. 17-2, 584 U.S. (2018).
[130] H.R.4943 - *The Clarifying Lawful Overseas Use of Data Act* (also known as CLOUD Act), 6 February 2018.

In response to this uncertainty, the "Clarifying Lawful Overseas Use of Data Act" (CLOUD Act) was passed on 23 March 2018.[131] The CLOUD Act specifies that all of the 1986 SCA's provisions on required disclosure apply regardless of the location of the communications or records.

The CLOUD Act, however, does allow for the network provider to object to a request for the contents of a communication (but not non-content data or subscriber information) based on comity grounds. As a prerequisite for the comity analysis of whether to defer to the foreign jurisdiction, the court must find that: (1) the subscriber being investigated is not a US citizen and does not reside in the US; and (2) turning over the information to U.S. law enforcement would "cause the provider to violate the laws of a qualifying foreign government".

A "qualifying foreign government" is defined largely as a function of whether a government has in place an executive agreement with the US governing access to data that meets a number of criteria as certified by the Attorney General, in concurrence with the Secretary of State. These criteria seek to guarantee most importantly that:

1. access to data is based on an order granted by a court or independent authority which seeks the data in connection with "the prevention, detection, investigation, or prosecution of serious crime, including terrorism" and which is based on "requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigations";
2. US persons or persons located in the United States shall not be the targets of any such surveillance orders and procedures shall be implemented, analogous to those which exist under FISA (discussed below), to minimize the acquisition, retention, and dissemination of information concerning U persons;
3. The country must meet international privacy and civil liberties standards;
4. The agreement "shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data";
5. The foreign government "shall afford reciprocal rights of data access, to include where applicable, removing restrictions on communications service providers, including providers subject to United States jurisdiction" which will allow them to respond to legal requests for data access, even if the jurisdiction's law would otherwise forbid it.

Such an executive agreement entitles the foreign government not only to the comity analysis exempting the data from disclosure to US prosecutors, but, more importantly, allows them to obtain personal data directly from ISPs, who are subject to US jurisdiction since they are headquartered in the US, but who operate communications networks and hold data of relevance to foreign criminal investigations abroad.

[131] For a comment see Mulligan, S.T. (2018), *Cross-border Data Sharing under the Cloud Act*, Congressional Research Service, R45172, 23 April.

The CLOUD Act establishes a direct conflict with EU data protection provisions. In fact, by virtue of Article 48 GDPR: "[a]ny judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter."

The CLOUD Act's unilateral assertion of jurisdiction over personal data located in the EU directly controverts this baseline principle of extraterritorial transfer to public authorities based on an international agreement. For such transfers to be lawful under EU law, it will therefore be necessary to use the possibility of entering into an EU-US executive agreement, which could then serve as the legal basis for transfers by network providers like Microsoft to US authorities.

Firstly, the law would clarify that a warrant issued under the Stored Communications Act 1986 does apply to data overseas, but it would also allow companies such as Microsoft to challenge warrants if they violate the law of the country where the data is hosted. Secondly, the bill would allow the US president to enter into "executive agreements" with other countries, and thus authorise foreign governments to seize data hosted in the US, without following its privacy legislation, so long as they are not targeting a US citizen, or an individual located within the United States. Such discretional power is, of course, very controversial.

5. Concluding Remarks

The report has briefly explored models of law enforcement access to personal data, identifying fundamental rights challenges at stake. It provided an overview of how primary and secondary law have evolved to allow cross-border access and exchange data for law enforcement purposes, on the one side, and ensure respect of fundamental rights, on the other side. It then addressed main controversies dealt with by landmark rulings of the CJEU and the ECtHR in this context. Finally, it elaborated upon current developments either in law or case-law which are likely to further influence the state of the art, including the transatlantic dimension of the issue.

The EU has privileged over the years a mediated access model for the cross-border exchange of information, whereby access to data is supervised by the designated authority and an independent court/tribunal of the requested country. The latest development in this is the European Investigation Order, which is a major advancement.

Yet we are gradually shifting towards unmediated access practices, whereby an authority in the requesting foreign country communicates its demands directly to the private company holding or controlling the data. In fact, the EPO proposals witness an additional shift away from traditional MLA agreements, involving the "direct" cooperation between law enforcement authorities seeking to obtain electronic evidence and the foreign service providers in (exclusive) control of it. Such mechanisms constitute a *de facto* extraterritorial reach of national investigative powers, and an extension of the "sword" function of criminal law via the further privatization of security.

Case-law and legislative developments on the other side of the Atlantic have deeply influenced such developments. It remains to be seen now how the EPO negotiations will evolve and where unmediated cross border access to information will go, with all the concerns it generates with reference to the protection of individual rights.

References

Aalto, P. et al. (2014), "Article 47 – Right to an Effective Remedy and to a Fair Trial", in Peers, S. et al (eds.), *The EU Charter of Fundamental Rights: A Commentary,* Oxford: Hart Publishing.

Allegrezza, S. (2014), "Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality", in Ruggeri, F. (ed.), *Transnational Evidence and Multicultural Inquiries in Europe,* Springer, p. 51–67.

Armada, I. (2015), "The European Investigation Order and the Lack of European Standards for the Gathering of Evidence. Is a Fundamental Rights-Based Refusal the Solution?", *1 New Journal of European Criminal Law*, p. 8-31.

Bachmaier, L. (2016), "Access to Telecommunication Data in Criminal Justice: Spain*",* in *Access to Telecommunication Data in Criminal Justice,* Berlin: Duncker & Humblot.

Bachmaier, L. (2017), "Mutual recognition and cross-border interception of communications: the way ahead of the European Investigation Order" in C. Brière and A. Weyembergh (eds.) *The needles balances in EU criminal law: past, present and future*, Oxford: Hart.

Bachmaier, L. (2015), "Transnational Evidence: Towards the Transposition of the Directive 2014/41 Regarding the EIO", *EuCrim,* Vo. 2, p. 47-60.

Bachmaier, L. (2010), "European Investigation Order for obtaining evidence in the criminal proceedings: study of the Proposal for a European Directive", *Zeitschrift für Internationale Strafrechtsdogmatik (ZIS)* 9, p. 580-589.

Bignami, F. (2007), "Privacy and Law Enforcement in the European Union", *Chicago Journal of International Law,* Vo. 8, No. 1, p. 233-255.

Bigo, D. et al. (2013), "Mass Surveillance of Personal Data by EU Member States and its compatibility with EU Law", CEPS, Brussels.

Bigo, D. et al. (2014), "National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges", CEPS, Brussels.

Boehm, F. (2012), *Information sharing and data protection in the area of Freedom Security and Justice,* Berlin: Springer-Verlag Berlin Heidelberg.

Boehm, F. (2012), "Information sharing in the AFSJ", in Gutwirth, S. et al (eds.), *European data protection: in good health?*, Springer, p. 143-183.

Bräutigam, T. (2016), "The land of confusion: international data transfers between *Schrems* and the GDPR", in Bräutigam, T. and S. Miettinen (eds.), *Data protection, privacy and European regulation in the digital age*, Forum Iuris.

Brouwer, E. (2008), *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Martinus Nijhoff Publishers.

Brouwer, E. (2011), "Legal boundaries and the use of migration technology" in Dijstelbloem, H. and A. Meijer (eds.) *Migration and the new technological borders of Europe*, Palgrave.

De Busser, E. (2016), "Private Companies and the Transfer of Data to Law Enforcement Authorities: Challenges for Data Protection", *Maastricht Law Journal.* Vo. 23, Issue 3, p. 479.

Carrera, S. et al. (2015), *Access to Electronic Data by Third- country Law Enforcement Authorities, Challenges to EU Rule of Law and Fundamental Rights*, CEPS, Brussels.

Carrera, S. and E. Guild (2016), "The End of Safe Harbor: What Future for EU-US Data Transfers?", *Maastricht Journal of European and Comparative Law,* Vo. 22, Issue 5, p. 651.

Carrera, S. and V. Mitsilegas (eds.) (2017), *Constitutionalising the Security Union*, CEPS, Brussels.

Cocq, C. (2016), "EU Data Protection Rules to Law Enforcement Activities: Towards a Harmonised Legal Framework?", *New Journal of European Criminal Law*, Vo. 7, No. 3, p. 263.

Curtin, D. (2015), "Data Privacy Rights and Democracy: Ireland, Europe and Beyond", *Irish Journal of European Law,* Vo. 18, No. 2, p. 5-14.

Daniele, M. (2015), "Evidence Gathering in the Realm of the EIO. From National Rules to Global Principles", *New Journal of European Criminal Law,* Vo. 2, p. 179.

Daskal, J. (2016), "Law enforcement access to data across borders: the evolving security and rights issues", *Journal of National Security Law & Policy,* Vo. 8, p. 473.

Daskal, J. (2015), "The Un-Territoriality of Data", *The Yale Law Journal,* Vo. 125, p. 326.

De Busser, E. (2009), *Data protection in EU and US criminal cooperation*, Antwerp: Maklu.

De Busser, E. (2013), "Privatisation of information and the data protection reform", in Gutwirth, S. et al (eds.), *Reloading data protection: Multidisciplinary Insights and Contemporary Challenges*, Springer, p. 129-149.

De Goede, M. (2012), *Speculative security: The Politics of Pursuing Terrorist Monies*, Minneapolis: University of Minnesota Press, p. 328.

De Hert, P. and V. Papakonstantinou (2016), "The New Police and Criminal Justice Data Protection Directive. A first analysis", *New Journal of European Criminal Law,* Vo. 7(1).

Digital Europe (2016), *Views on Law Enforcement Access to Digital Evidence*, Brussels, 17 October.

Feiler, L. (2010), "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection", *European Journal of Law and Technology,* Vo. 1(3).

Fenwick, H. (ed.) (2012), *Development in counter-terrorist measures and uses of technology,* Routledge.

Mouzakiti, F. (2015), "Transborder Data Flows 2.0: Mending the Holes of the Data Protection Directive", *European Data Protection Law Review,* Vo. 1, p. 39.

Forgó, N. et al (2017), "The Principle of Purpose Limitation and Big Data", in Forgó, N. et al (eds.), *New Technology, Big Data and the Law,* Springer, p. 17-42.

Davis, F.T. (2015), "A U.S. Prosecutor's Access to Data Stored Abroad – Are There Limits?", *The International* Lawyer, Vo. 49, No. 1.

Galli, F. (2016), "Digital Rights Ireland as an opportunity to foster a desirable approximation of data retention provisions", in Special Issue on "*A balanced data protection in the European Union*", *Maastricht Journal of European and Comparative Law,* Vo. 23, No. 3, p. 460.

González Fuster, G. (2014), *The emergence of personal data protection as a fundamental right of the EU*, Springer.

González Fuster, G., P. De Hert and S. Gutwirth (2008), "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law, Computers & Technology,* Vo. 22, No. 1, p. 191.

Granger, M.-P. and K. Irion (2014), "The Court of Justice and the Data Retention Directive in *Digital Rights Ireland*", *European Law Review, Vo.* 39, No. 6, p. 836.

Guild, E. and S. Carrera (2014), "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", *Paper in Liberty and Security in Europe,* CEPS, Brussels, No. 65, May.

Guild, E. and S. Carrera (2014), "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", CEPS, Brussels.

Hijmans, H. and A. Scirocco (2009), "Shortcomings in EU Data Protection in the Third and the Second Pillars: Can the Lisbon Treaty Be Expected to Help?", *Common Market Law Review,* Vo. 46, p. 1485.

Hustinx, P. (2017), "EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation", in Cremona, M., *New technologies and EU law,* OUP.

Irion, K. (2015), "Accountability unchained: Bulk Data Retention, Pre-emptive Surveillance, and Transatlantic Data Protection", in Rotenberg, M., et al (eds.), *Visions of Privacy in the Modern Age,* New York: New Press.

Kessler, D. et al (2016), "The potential impact of art 48 of the General Data Protection Regulation on cross border discovery from the United States", *The Sedona conference Journal*, Vo. 17, No. 2, p. 575.

Klip, A. (2013), *European criminal law. An integrative approach,* Intersentia, 3rd edition.

Kosta, E. and P. Valcke (2006), "Retaining the Data Retention Directive", *Computer Law and Security Report,* Vo. 22, No. 5, p. 370.

Kris, D. (2015), "Preliminary Thoughts on Cross Border Data Requests", *Lawfare*, 28 Sept (http://www.lawfareblog.com/preliminary- thoughts-cross-border-data-requests).

Krzysztofek, M. (2017), *Post-reform personal data protection in the European Union: general data protection regulation (EU) 2016/679,* Wolters Kluwer.

Kuner, C. (2014), "A "Super-right' to data protection? The Irish Facebook Case and the future of the EU data transfer regulation", *Concurring Opinions (Blog).* (http://concurringopinions.com/archives/2014/06/the-data-retention-judgment-the-irish-facebook-case-and-the-future-of-eu-data-transfer-regulation.html).

Kuner, C. (2009), "Developing an adequate legal framework for international data transfers", in S. Gutwirth et al (eds.), *Reinventing data protection?*, Springer, p. 263-273.

Lachmayer, K. (2015), "Rethinking privacy beyond borders", *Tilburg Law Review,* Vo. 20, p. 78.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, OUP.

Mangiaracina, A. (2014), "A New and Controversial Scenario in the Gathering of Evidence at the European Level: The Proposal for a Directive on the European Investigation Order", *Utrecht Law Review,* Vo. 10, No. 1, p. 113.

Mitsilegas, V. (2009), *EU Criminal Law*, Hart.

Mitsilegas, V. (2009), "The Borders paradox: the surveillance of movement in a Union without internal frontiers", in *A right to inclusion and exclusion: Normative Fault lines of the EU's AFSJ*, Hart.

Mitsilegas, V. (2006), "The Constitutional Implications of Mutual Recognition in Criminal Matters in the EU", *Common Market Law Review, Vo.* 43, p. 1277.

Mitsilegas, V. et al. (2014), "The End of the Transitional Period for Police and Criminal Justice Measures Adopted before the Lisbon Treaty: Who Monitors Trust in the European Justice Area?", CEPS, Brussel.

Mitsilegas, V. (2016), *EU criminal law after Lisbon,* Hart.

Mitsilegas, V. (2003), "The New EU-US Co-operation on Extradition, Mutual Legal Assistance and the Exchange of Police Data", *European Foreign Affairs Review,* Vo. 8, p. 515.

Mitsilegas, V. (2012), "The Limits of Mutual Trust in Europe's Area of Freedom, Security and Justice. From Automatic Inter-state Cooperation to the Slow Emergence of the Individual", *Yearbook of European Law,* Vo. 31, 319.

Mitsilegas, V. and N. Vavoula (2017), "The normalisation of surveillance of movement in an era of reinforcing privacy standards", in Bourbeau, P. (eds.), *Handbook on Migration and security*, Elgar.

Mitsilegas, V. (2014), "Transatlantic counter-terrorism cooperation and European values", in Curtin, D., and E. Fahey (eds.), *A transatlantic community of law,* CUP, p. 289-315.

Mitsilegas, V. (2015), "The Transformation of Privacy in an era of pre-emptive Surveillance", *Tilburg Law Review,* Vo. 20, p. 35.

Ojanen, T. (2014), "Privacy Is More Than Just a Seven-Letter Word", *European Constitutional Law Review,* Vo. 10, No. 3, p. 528.

O'Neill, M. (2010), "The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar", *Journal of Contemporary European Research,* Vo. 6, No. 2, p. 211.

EDPS (2012), Opinion of the on the data protection reform package, 7.3.2012. (https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf)

Peers, S. et al. (eds.) (2014), *The EU Charter of Fundamental Rights: A Commentary*, Hart.

Roach, K. (2010), "The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations", in McGarrity, N. et al (eds.), *Counter-Terrorism and Beyond The Culture of Law and Justice After 9/11,* London: Routledge-Cavendish, p. 48-68.

Ruggeri, S. (2014), "Introduction to the Proposal of a European Investigation Oder: Due Process Concerns and Open Issues" in Ruggeri, S., (ed.), *Transnational Evidence and Multicultural Inquiries in Europe,* Springer, p. 29–35.

Sieber, U. and N. von Zur Mühlen (2016), *Access to Telecommunication Data in Criminal Justice. A comparative Analysis of European Legal Orders*, Duncker & Humblot.

Swire, P. and J. Hemmings (2016), "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program", *Georgia Tech Scheller Coll. Of Bus. Research Paper,* No. 38.

Tikkinen-Piri, C. et al (2017), "EU General Data Protection Regulation: changes and implications for personal data collecting companies", *Computer and Security Review*, No. 1.

Van Hoek, A. and M. Luchtman (2005), "Transnational cooperation in criminal matters and the safeguarding of human rights", *Utrecht Law Review, Vo.* 1, No. 2.

Vavoula, N. (2016), Immigration *and privacy in the law of the EU: the case of databases*, PhD thesis (Publication forthcoming), Queen Mary University of London.

Vermeulen, G. (2016), "The Paper Shield", in Svantesson, D. and D. Kloza (eds.), *Transatlantic data privacy relationships as a challenge for democracy*, Intersentia.

Voigt, P. (2017), *The EU General Data Protection Regulation (GDPR) A Practical Guide*, Springer.

Zimmermann, F. et al (2011), "Mutual Recognition and its Implications for the Gathering of Evidence in Criminal proceedings: a Critical Analysis of the Initiative for a European Investigation Order", *European Criminal Law Review,* No. 14, p. 56.

Zerbes, I. (2015), “Legal Issues of Transnational Exchange of Electronic Evidence in Criminal Proceedings” *European Criminal Law Review,* No. 3, p. 304.