



Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters

State of the art and latest developments in the EU and the US

Marco Stefan and Gloria González Fuster

No. 2018-07, November 2018

Abstract

In the digital age, access to data sought in the framework of a criminal investigation often entails the exercise of prosecuting powers over individuals and material that fall under another jurisdiction.

Mutual legal assistance treaties, and the European Investigation Order allow for the lawful collection of electronic information in cross-border proceedings. These instruments rely on formal judicial cooperation between competent authorities in the different countries concerned by the investigative measure. By subjecting foreign actors' requests for data to domestic independent judicial scrutiny, they guarantee that the information sought during an investigation is lawfully obtained and admissible in court.

At the same time, pressure is mounting within the EU and in the US to allow law enforcement authorities' access to data outside existing judicial cooperation channels. Initiatives such as the European Commission's proposals on electronic evidence and the CLOUD Act in the US foster a model of direct private–public cross-border cooperation under which service providers receive, assess and respond directly to a foreign law enforcement order to produce or preserve electronic information.

This paper scrutinises these recent EU and US initiatives in light of the fundamental rights standards, rule of law touchstones, and secondary norms that, in the EU legal system, must be observed to ensure the lawful collection and exchange of data for criminal justice purposes. A series of doubts are raised as to the Commission e-evidence proposal and the CLOUD Act's compatibility with the legality, necessity and proportionality benchmarks provided under EU primary and secondary law.



This paper 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.

CEPS Papers in Liberty and Security in Europe offer the views and critical reflections of CEPS researchers and external collaborators on key policy discussions surrounding the construction of the EU's Area of Freedom, Security and Justice. The series encompasses policy-oriented and interdisciplinary academic studies and comment on the implications of Justice and Home Affairs policies within Europe and elsewhere in the world.

Marco Stefan is a Research Fellow within the Justice and Home Affairs Section at CEPS. Gloria González Fuster is a Research Professor and a member of the Law, Science, Technology & Society Research Group at the Vrije Universiteit Brussel. The authors would like to express their gratitude for the invaluable comments and input by Sergio Carrera, Senior Research Fellow and Head of the Justice and Home Affairs Section at CEPS.



Contents

Executive summary	i
1. Introduction	1
2. EU primary law standards and cross-border access to data for criminal justice purposes.....	4
2.1. Privacy and criminal justice standards.....	4
2.2. The role of independent judicial scrutiny in cross-border criminal proceedings.....	7
3. EU secondary law on cross-border evidence gathering for criminal justice purposes....	12
3.1. Mutual legal assistance and the EU legal framework for transatlantic data transfer in criminal proceedings	13
3.2. The European Investigation Order	19
4. The European Commission's e-evidence proposals	24
4.1. Background of the proposals	25
4.2. The e-evidence proposals in light of EU primary and secondary law standards....	27
4.2.1. The right legal basis? Criminal justice vs police cooperation	27
4.2.2. Concerns over necessity, legality and proportionality.....	30
4.2.3. Issues arising from the execution, review and enforcement of the proposed orders	33
4.2.4. Effectiveness and accessibility of remedies under the European Production and Preservation Order proposals.....	39
4.2.5. EU privacy and data protection safeguards	40
5. Concluding remarks	45
Glossary	48
References	51

List of Figures and Tables

Figure 1. US processing of EU Member State MLA requests for data	14
Figure 2. Execution of an EIO	20
Figure 3. Execution and enforcement of the proposed orders	34
Table 1. Personal scope (e-evidence proposals and the CLOUD Act).....	25
Table 2. Standards applying to the issuing of Production Orders.....	31

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
ECHR	European Convention on Human Rights
ECPA	Electronic Communications Privacy Act
ECtHR	European Court of Human Rights
EIO	European Investigation Order
EPOC	European Production Certificate
EPOC-PR	European Preservation Order Certificate
EU Charter	European Union Charter of Fundamental Rights
GDPR	General Data Protection Regulation
IP	Internet protocol
LEAs	Law enforcement authorities
MLA	Mutual legal assistance
MLAT	Mutual legal assistance treaty
OTT	Over the top (Communication Service Providers)
SCA	Stored Communications Act
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

Executive summary

EU standards applying to cross-border access to electronic data

Access to electronic information for criminal law enforcement purposes constitutes an intrusive investigative measure that is likely to affect the fundamental rights of individuals. Given the transnational dimension of the internet, law enforcement quests for data also poses a series of jurisdictional challenges. Prosecuting authorities' demands for information held by private companies and stored abroad, or in the cloud, often affect rules and responsibilities of other states concerned by the execution of the foreign investigative measure. Practice has shown how conflicts of law arise when law enforcement actors assert their powers over individuals and data that fall under another jurisdiction.

In the post-Lisbon Treaty framework, regulating the access to and sharing of information in the fight against terrorism and crime is no longer an exclusive prerogative of Member States, but fall squarely within domains of competence (i.e. police and judicial cooperation in criminal matters) that are shared with the EU. The EU has progressively developed an EU criminal justice area that also addresses the gathering of data for purposes related to the prevention, detection, investigation and prosecution of crime. As a consequence, EU Member States have the obligation to ensure that domestic *and* foreign authorities' cross-border access to and transfers of data are compatible with the fundamental rights and rule of law standards provided in the EU legal system.

EU primary law guarantees the rights to privacy (Article 7 EU Charter) and data protection (Article 8 EU Charter), as well as a set of criminal justice safeguards (Articles 47-50 EU Charter). Constitutional specificities and different legal traditions of EU countries provide further limits to criminal justice and law enforcement cooperation. These national and supranational standards must be adhered to by Member States, third countries, as well as private companies addressed by law enforcement authorities seeking EU data, regardless of factors such as the nationality of the data subject or the place of establishment of the service provider holding the data sought.

Independent judicial oversight is necessary to ascertain that in the extraterritorial exercise of their criminal jurisdiction, foreign authorities remain bound by EU primary and secondary law, and respect national constitutional and criminal law. The case law of the Court of Justice of the European Union shows that this responsibility relies upon both the judicial authority issuing or validating a decision to enforce criminal jurisdiction across borders, *and* the courts of the EU country where such a cross-border law enforcement measure is to be executed.

In fact, EU Member States' criminal justice systems perform differently under important judicial independence indicators. Lack of judicial independence and '*prosecutorial bias*' in issuing countries entail the risks of quasi-automatic approval of all data requests from the prosecutors, and constitute a danger not only for the fundamental rights of the persons concerned, but also for the independence of the judiciary and the EU rule of law as a whole.

EU legal framework for judicial cooperation on evidence gathering

EU legal instruments for channelling cross-border requests for data gathering in criminal proceedings currently encompass mutual legal assistance treaties (MLATs) and the European Investigation Order (EIO). The EIO Directive only entered into force in May 2017, and its transposition in Member States' national legislation is very recent.

To date, a knowledge gap exists as to the exact ways in which this EU legal instrument and MLA agreements are implemented in judicial and administrative practices across EU Member State, as well as in bilateral cooperation frameworks with key international partners. That notwithstanding, the legal benchmarks provided under MLATs and the EIO cannot simply be disregarded by the EU or its Member States when undertaking further internal or external initiatives on data collection for criminal justice purposes.

EU MLATs and the EIO rely on a model of formal judicial cooperation that subjects cross-border access and exchange of data to systematic independent judicial scrutiny. Such scrutiny is conducted in both the state seeking the information *and* the country where the investigative measure has to be executed. By ensuring that the right authorities are involved and that appropriate EU and national safeguards are taken into account, MLATs and the EIO allow the lawful collection of data across borders, and guarantee that the data obtained abroad are effectively admitted as evidence before the courts of the prosecuting state.

The EIO, in particular, is intended to streamline and speed up judicial cooperation for access to data by extending the principle of mutual recognition to the field of evidence gathering in criminal proceeding. At the same time, it also calls upon the judicial authorities in the executing state to verify whether specific grounds of legitimate refusal to recognise and execute an EIO exist. These grounds, which are assessed *before* access to data is granted, are not limited to fundamental rights and conflict of law considerations, but also encompass cases where the execution of an EIO could lead to a breach of rules on immunity or privilege, or rules limiting criminal liability relating to freedom of the press, or where it could harm essential national security interests, or infringe the *ne bis in idem* principle.

Introduction of direct cooperation instruments

In the EU and the US, a number of initiatives are being developed to allow law enforcement authorities gather data *outside* the judicial cooperation channels provided by the MLATs and EIO. Initiatives such as the US Clarifying Lawful Use of Overseas Data (CLOUD) Act, and the Commission's proposals on e-evidence would allow law enforcement actors, and in particular police and prosecutors, to serve upon service providers orders directed at obtaining the disclosure and retention of data. The achievement of this goal will depend on the establishment of a "new" public-private framework of direct cooperation where service providers' compliance with the orders is required, regardless of the location of the data solicited. In reality, such a method of direct cooperation is already followed in practice by certain countries.

US authorities, in particular, have consistently bypassed MLA channels to request data held by US companies abroad, including in the EU. The legality of the US authorities' practice to order private companies to disclose data stored in the EU has been famously challenged in the *Microsoft Ireland* case. The dispute essentially questioned the lawfulness of extraterritorial assertion of US criminal jurisdiction in light of standing (i.e. pre-CLOUD Act) US legislation. The question, however, was far from being an exclusively domestic one. Foreign authorities' unmediated access to data stored in the EU raises far-reaching issues also from the EU law perspective.

The CLOUD Act

Part I of the CLOUD Act formally grants US LEAs the power to order US private companies abroad to disclose the "content of a wire or electronic communication and any record of other information". Part II paves the way for "executive agreements" that, when concluded, would allow non-US governments to directly request data of non-US persons from US-based companies. From an EU law perspective, a number of questions arise with regard to the CLOUD Act's fitness to provide a sound legal basis for the gathering and transfer of data in the context of cross-border criminal proceedings.

Doubts exist as to the possibility for US service providers located in the EU to transfer data exclusively based on warrants issued under the CLOUD Act, meaning outside any EU international agreement or legally binding instrument in force between the parties. The scope of having EU rules on cross-border transfers of personal data apply to a non-EU state is precisely to avoid that in the extraterritorial application of their domestic law, foreign authorities hamper the attainment of the protection that in the Union is granted to all natural persons.

It is true that Article 49 of the General Data Protection Regulation allows for the possibility to derogate from mutual legal assistance processes. However, this provision does not seem to provide an appropriate EU legal basis to justify all transfers of data ordered by the US under the CLOUD Act, as such a norm permits data transfers "only if the transfer is not repetitive" and it "concerns only a limited number of data subjects", in addition to needing to be accompanied by specific suitable safeguards. Under the CLOUD Act, US law enforcement authorities are instead given unlimited jurisdiction over any data (including content, metadata and subscriber information) controlled by US companies abroad.

With regard to Part II of the CLOUD Act, serious doubts emerge as to the possibility for individual EU Member States to lawfully engage in the negotiation and conclusion of an executive agreement that would allow them to cooperate bilaterally in a field where the Union has undertaken extensive internal and external action. A fundamental EU law compatibility issue would arise also with regard to the disparity in the guarantees that under any given CLOUD Act executive agreement would be granted, on the one hand, to 'United States persons' and, on the other hand, to persons from the rest of the world – including EU citizens, and more generally anybody whose data must be protected under the EU Charter.

Any further initiative between the EU and the US would need to take into account the benchmarks of judicial cooperation provided under the MLA system. Exercising *reciprocal* judicial scrutiny over incoming LEA requests for data emerges in particular as an essential requirement under EU law. On the one hand, such scrutiny enables the protection of the subject whose data fall under EU law, as confirmed by the fact that under the EU–US MLA Agreement requests issued by US authorities directed at obtaining data stored in the EU by non-US companies have been refused on grounds such as the absence of dual criminality, a failure to demonstrate a nexus between the evidence sought and the criminal conducted alleged, and on the basis of essential interests. On the other hand, it serves the purpose of ensuring that EU citizens’ fundamental rights are appropriately guaranteed in the US.

Proposals for European Production and Preservation Orders

In April 2018, the European Commission tabled two legislative proposals on ‘electronic evidence’ (e-evidence) in criminal matters. The first is a proposal for a regulation that foresees the introduction of two new data-gathering tools, namely the European Production and Preservation Orders. The second consists of a proposal for a directive that would introduce an obligation for private companies in the EU to appoint “at least one” legal representative to act as a point of contact for Production and Preservation Orders issued by Member State LEAs.

The proposed orders are qualified by the Commission as instruments of judicial cooperation in criminal matters. Accordingly, the legal basis selected for the proposed e-evidence regulation is Article 82(1)(d) of the Treaty on the Functioning of the European Union. This choice is questionable, as it does not seem to appropriately reflect the *aim* and *content* of the proposed measure. In fact, rather than promoting cooperation between judicial authorities of different Member States, the proposal seems to be concerned with the establishment of a public–private framework of cooperation under which service providers receive, assess and respond directly to foreign law enforcement requests to produce or preserve data, and are subject to sanctions in case they do not comply with an Order.

The Commission claims that the ‘orders’ would bring into being a ‘new model’ of mutual recognition. However, EU primary law circumscribes the application of mutual recognition instruments to cooperation between *competent Member State authorities*. In particular, under existing mutual recognition procedures (and in particular the EIO), the execution of other Member States’ orders always *requires the prior involvement of a judicial authority* in the Member State where the addressee or the object concerned by the measure is located.

Ascription of judicial authorities as the depositary of trust in EU criminal matters ultimately depends on the division of powers principle, which presumes their structural independence in assessing whether the execution of another Member State’s order will not infringe EU principles, laws and values. To the contrary, there is no general assumption of reciprocal trust between public authorities and private companies.

That notwithstanding, the proposed Regulation fails to ensure systematic independent judicial oversight, as it does not require independent judicial oversight in the country issuing the orders when these target specific categories of *supposedly* ‘less sensitive’ data (i.e. subscriber and access data). Also, the involvement of the competent judicial authorities of the Member State where the data or the company holding it is located is only *eventual* and *accidental*, being foreseen for solely in cases where the *service provider* decides not to execute the order. Under EU law, the competent judicial authorities of the country where the investigative measure should be executed have the duty not to do so when a refusal is justified by considerations related to *inter alia* fundamental rights concerns and/or the incompatibility of the order with the criminal justice standards provided by EU *and* domestic law.

In a context where no systematic involvement of judicial authorities is ensured in relation to the *ex ante* assessment of the orders, the service provider might well be forced to execute an order that is not only unlawful under the law of the country where it is located (or represented), but also possibly incompatible with relevant provisions of the legal system of the issuing Member State. At the same time, the possibility of a company not objecting to a request for data when it should do so might undermine the very objective of the proposed measure, which is to allow data obtained across borders to be admitted as evidence before courts.

Assessing the lawfulness of a cross-border investigative measure is simply not part of the statutory goals of private organisations that pursue exclusively commercial interests. Only independent judicial authorities possess the necessary institutional prerogatives and professional capacity to ensure an appropriate scrutiny of whether a legitimate ground subsists for refusing the execution of another Member State’s criminal law enforcement measure. Independent judicial oversight is also required to ensure that the legitimate interest of service providers in complying with a foreign authority’s order to transfer data sought in the framework of a criminal investigation does not override the interests or fundamental rights and freedoms of the data subject.

A series of doubts also emerge with regard to the compatibility of the European Production and Preservation Orders with the principles of necessity and proportionality. The Commission proposes that these measures are issued for all types of crimes (and without prior independent judicial validation) when subscriber and access data are sought. There is a risk of legalising ‘fishing expeditions’ whereby investigators order service providers to produce or preserve large troves of non-content data. When used to obtain content or transactional data, the new instruments could also lead to a problematic increase in the administrative burden in national judicial systems of the issuing states, with judges being potentially exposed to a large number of ‘orders’ to review.

Furthermore, large discretion is left to individual Member States in establishing the different categories of crimes for an order related to the production of content and transactional data. The proposal could thus enable data processing in an unforeseeable manner across the Union, which would be in direct tension with EU fundamental rights requirements and the need to maintain mutual trust within the EU criminal justice area.

Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters

Marco Stefan and Gloria González Fuster

CEPS Paper in Liberty and Security in Europe No. 2018-07, November 2018

1. Introduction

The exponential use of internet services for daily communications and activities has led law enforcement authorities (LEAs)¹ to increasingly rely on the access to and collection of electronic information for the investigation and prosecution of crime.

Data transmitted in digital form and stored by private service providers² in different countries are often considered valuable, if not indispensable, probatory sources. Granting law enforcement actors the possibility to swiftly gather different types of electronic data³ across borders is considered crucial not only for the countering of ‘cybercrime’ (both target and content-related), but also for the investigation and prosecution of criminal offences in the ‘offline world’.⁴

While working towards the establishment of an area of freedom, security and justice (AFSJ), the EU has progressively developed an EU criminal justice area. The latter addresses different aspects of intra-EU and international cross-border judicial cooperation in criminal matters, including investigative measures aimed at gathering evidence abroad. EU instruments for judicial cooperation in criminal matters provide investigating and prosecuting authorities with the possibility to issue requests directed at obtaining pieces of information, also in digital form, which are held by foreign service providers and/or located in another Member State within the Union, or in third countries such as the US.

These instruments currently encompass mutual legal assistance treaties (MLATs), which represent the ‘classic’ international law instrument used for channelling cross-border requests for evidence gathering in criminal proceedings, and the European Investigation Order (EIO), which can be used to carry out investigative measures within the EU, based on the principle of mutual recognition of judicial decisions. Both the MLATs and the EIO adopt a mediated model for law enforcement cross-border access to electronic information that relies on formal judicial cooperation between pre-identified competent authorities in the different countries concerned (Carrera et al., 2015). This means that MLATs and the EIO subject cross-border

¹ See the glossary in this report.

² Ibid.

³ Ibid.

⁴ From the perspective of the authority requesting the data, the cross-border element might depend on different factors, including the location of the data, the place where service providers have their main site or any other establishment and the place where the service provider offers services. The nationality and residence of the suspect and/or the victim also contribute to the cross-border and cross-jurisdictional nature of a request for data. See Internet & Jurisdiction Policy Network (2017), p. 10.

access and exchange of information for criminal justice purposes to independent judicial scrutiny in both the state seeking the information and the country where the final subject of the order is located.

The ex ante involvement of independent judicial authorities is designed to *prevent* possible conflicts of law and jurisdictions that often arise when LEAs assert their powers abroad. Judicial scrutiny serves the purpose of mutually verifying that requests for access to data are consistent with the national, international and supranational standards and provisions respectively applying to the issuing and execution of cross-border investigative measures. For EU Member States, these standards and provisions are not just confined to domestic law, but also include EU rules and values. Since the entry into force of the Lisbon Treaty, EU countries have in fact had the responsibility to ensure that other EU Member States or third countries' law enforcement actions performed in their territory or under their jurisdiction are compatible with EU law (Mitsilegas, 2016).

Despite the existence of successful examples of cooperation under the mutual legal assistance (MLA) system (Bass, 2015; Kendall and Funk, 2014), and the EIO having entered into force only in May 2017 (that is, very recently), it is ever often argued that this model of formal judicial cooperation is 'outdated', and therefore 'ineffective', when it comes to the collection of data in the fight against crime (Swire et al., 2017, p. 324). Claims are made that the gathering of data for criminal justice purposes presents specific operational challenges that do not affect other investigative measures. These challenges would mainly derive from the 'volatility' of electronic information, because of which LEAs' access to data under the jurisdiction of another state cannot be delayed by the cross-border and trans-jurisdictional nature of the request.⁵

Current critiques of the MLATs and the EIO model focus on the delays associated with the obligation to subject cross-border requests for data to foreign judicial scrutiny. Repeated calls have subsequently been made to remove "obstacles to criminal investigations" in cyberspace,⁶ in particular those stemming from standing EU (EIO) and international (MLA) rules on judicial cooperation for access to electronic information held by service providers. The underlying assumption is that the prosecution of crime could improve drastically in a context where law enforcement actors could attain electronic information directly from the service providers holding them, and without first having to obtain an authorisation from the judicial authorities of the country where the company holding the data is located.

Nevertheless, far-reaching issues arise from the implementation of this cooperation model, which in practice allows law enforcement actors to request or even order service providers to disclose data stored abroad. The risk is that the execution of such a request or order violates the (national or supranational) law applying in the country concerned. The jurisdictional, legal and practical challenges that come from directly (i.e. non-judicially mediated) sending requests

⁵ European Commission (2018a), p. 20.

⁶ European Commission (2015).

for access to electronic information held by service providers were made manifest in the long-running dispute underlying the *Microsoft Ireland v Department of Justice* case.⁷

The case originated in Microsoft's refusal to execute a US warrant to disclose some data stored in the EU. This type of extraterritorial exercise of criminal jurisdiction is a longstanding practice of US LEAs.⁸ However, in the specific case the company challenged the US warrant's power to reach overseas data. As discussed in section 3, the case, which had been pending appeal before the US Supreme Court, was ultimately dismissed. Meanwhile, policy and legislative efforts have been directed at the creation of new data-gathering tools for crime fighting across the Atlantic, but also within the EU. In the US, the signature of the Clarifying Lawful Use of Overseas Data (CLOUD) Act⁹ constituted a significant step in that direction.

Days after the CLOUD Act was passed by US Congress, the European Commission tabled two legislative proposals on 'electronic evidence' (e-evidence) in criminal matters. The first is a proposal for a regulation¹⁰ that introduces two new data-gathering tools, namely the European Production Order and the Preservation Order. The second consists of a proposal for a directive¹¹ that would introduce an obligation for service providers in the EU to appoint "at least one" legal representative to act as a point of contact responsible for receiving and executing Production and Preservation Orders issued by Member State LEAs.

The CLOUD Act and the Commission's proposals on e-evidence present their own differences and specificities, but they both espouse the model of so-called direct cooperation between law enforcement actors and service providers. These new measures aim at equipping prosecuting authorities with the power to obtain data directly from service providers, without going through pre-established channels of judicial cooperation. Since they represent a radical departure from the legal framework of cooperation established under the MLATs and the EIO, careful scrutiny is needed in order to verify their coherence with EU primary and secondary rules governing the collection and exchange of data for law enforcement purposes within the EU and in relation with third countries.

One of the aims of the JUD-IT project is to identify the substantive and procedural standards that – in a post-Lisbon Treaty framework – govern cross-border access to electronic data for criminal justice purposes. In this vein, this state-of-the-art report undertakes the following:

- i) it identifies the EU constitutional fundamental rights and rule of law safeguards that must be incorporated into EU (internal and external) criminal justice instruments

⁷ *Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.* 3. 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

⁸ Stored Communications Act (SCA), codified at 18 U.S.C. Chapter 121 §§ 2701–2712. Under the SCA, US law enforcement actors are authorised to compel US providers to disclose information about a person, regardless of both the nationality of the data subject and the localisation of the data.

⁹ Clarifying Lawful Overseas Use of Data (CLOUD Act), S. 2383, H.R. 4943.

¹⁰ European Commission (2018c), hereinafter, the 'proposed Regulation'.

¹¹ European Commission (2018c), hereinafter, the 'proposed Directive'.

regulating the gathering and exchange of data held by private companies. Attention is especially given to the conditions to be met in order to ensure adequate levels of privacy and data protection as well as effective judicial remedies vis-à-vis prosecuting authorities seeking access to electronic information in the context of criminal proceedings. These are key requirements that must be satisfied for law enforcement access to data to be legal under EU law (section 2);

- ii) analyses how and to what extent the EU primary law standards have been embedded in existing criminal justice instruments for cross-border cooperation in the field of evidence gathering. In particular, an overview is provided of the ways in which the EU MLATs and the EIO function as avenues of criminal justice cooperation that, while enabling data gathering across borders, also respond to issues concerning conflicts of law, mutual trust and fundamental rights compliance, proportionality and domestic constitutional specificity, and protection of citizens before third countries (section 3); and
- iii) provides a preliminary qualitative assessment of the Commission's proposals on e-evidence in light of EU primary and secondary law standards. A set of critical questions is posed with regard to the legal basis chosen for the proposals. In relation to the content of the latter, particular attention is paid to legality, necessity and proportionality aspects, as well as to issues of compliance with EU rules on privacy and data protection. Thought is also given to the legal and practical challenges that would arise from the execution, enforcement and review of the proposed European Production and Preservations Orders (section 4).

The research conducted for this report is intended to lay the groundwork for more in-depth analysis and for the development of further expert discussions as part of the JUD-IT project. Information collected and analysed for this report was obtained through desk research. To complement and validate the research, 16 face-to-face semi-structured interviews were held between May and September 2018 with relevant stakeholders. The latter included officials from the European Commission and Member States, US government representatives, civil society actors, service providers and legal practitioners as well as academics based in Brussels and Washington.

2. EU primary law standards and cross-border access to data for criminal justice purposes

2.1. Privacy and criminal justice standards

In the post-Lisbon Treaty framework, rules on the access to and sharing of information in the fight against terrorism and crime are no longer an exclusive prerogative of Member States, but fall squarely within areas of competence (i.e. police and judicial cooperation in criminal matters) that are shared with the EU.

The ‘Lisbonisation’ of the AFSJ granted a full role to the European Commission in enforcing EU legal standards in these domains, provided for their democratic scrutiny by the European Parliament, and entrusted the monitoring of their effective implementation to judicial control. The latter is performed by the Court of Justice of the European Union (CJEU), as well as EU Member States’ competent courts.

Depending on whether access to electronic data is conducted for the purpose of policing activities¹² or for formal judicial proceedings in criminal matters,¹³ particular sets of EU rules apply. The specific and practical aim along with the content of instruments regulating cross-border access to data is central to determining their pertinent legal basis, as well as to identifying the corresponding regulatory framework to take into account in their design and implementation.¹⁴

The JUD-IT project focuses on the standards and rules that concern the gathering and exchange of data for criminal justice purposes (i.e. in the context of criminal proceedings). That notwithstanding, it is important to recall that a number of EU primary law safeguards apply across all areas of EU law, including those referred to in Title V of Part Three of the Treaty on the Functioning of the European Union (TFEU) and relating to the AFSJ.¹⁵ Their consistent application to all activities entailing access to and exchange of data in the fight against crime is required to prevent that such initiatives translate into arbitrary or unjustified interferences with individuals’ rights.

Of special relevance in this context are the guarantees that the European Union Charter of Fundamental Rights (EU Charter) sets forth with regard to the right to respect for private life (Article 7) and the right to data protection (Article 8).¹⁶ These rights, which are distinct even though they can be described as mutually reinforcing each other (Mitsilegas and Vavoula 2018), fully apply to EU and Member State policies in the fields of police and judicial cooperation in criminal matters. The CJEU has made clear they need to be assessed also in conjunction with Article 47 of the Charter, on access to judicial remedies.¹⁷

The CJEU has progressively clarified that any limitation of the fundamental rights of respect for private life and data protection must be limited to what is strictly necessary, and outlined the implications of such a principle.¹⁸ The Court in Luxembourg also provided detailed guidance on how EU and Member States’ initiatives entailing the transfer of data across borders to third

¹² Article 82(21)(d) of the Treaty on the Functioning of the European Union (TFEU).

¹³ Article 87(2) TFEU.

¹⁴ See notably Opinion 1/15 of the Court (Grand Chamber) on the EU–Canada PNR Agreement, 26 July 2017 [ECLI:EU:C:2017:592].

¹⁵ As recognised in Declaration 21 of the Lisbon Treaty.

¹⁶ Article 16 TFEU and Article 39 of the Treaty on European Union provide new legal bases, which require that all EU policy areas, including law enforcement, ensure a comprehensive level of data protection.

¹⁷ See Case C-362/14, *Maximilian Schrems* [ECLI:EU:C:2015:650].

¹⁸ See Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [ECLI:EU:C:2014:238], and Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Tom Watson* [ECLI:EU:C:2016:970], para. 96.

countries, for purposes including the prevention, detection or prosecution of terrorist offences or serious transnational crime, must also be limited to what is strictly necessary, meaning the legislation entailing the limitation of the fundamental rights to the right to respect for private life and data protection must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse, and indicating, in particular, what circumstances and under which conditions a measure providing for the processing of such data may be adopted.¹⁹

When cross-border access to data by law enforcement is sought for a criminal investigation, it must also be compatible with EU criminal justice standards. These chiefly include the right to an effective remedy and to a fair trial, respect for the presumption of innocence and the right of defence, the principles of legality and proportionality of criminal offences and penalties, and the *ne bis in idem* principle (Articles 47–50 EU Charter).²⁰ Procedural guarantees embedded in national constitutional and criminal justice traditions provide further limits to criminal justice cooperation between EU Member State authorities (Cape et al., 2010). On several occasions, the constitutional courts in Member States have stressed that in the implementation of EU criminal justice measures (e.g. a European Arrest Warrant), national authorities cannot bypass other EU countries' constitutional checks and balances (Hong, 2016).

It is clear that the decision to issue cross-border requests for access to data largely depends on Member States' criminal law provisions. National legislation also outlines the procedural rules and identifies the oversight systems that apply to the issuing of cross-border requests for access to data. At the same time, the EU institutions and the Member States have the obligation to ensure that both domestic *and* foreign LEA requests for electronic data held by private companies do not expose individuals to the risk of violations of the fundamental rights they are entitled to under the EU Charter and national constitutions.

Therefore, if they are to comply with relevant fundamental rights and rule of law standards provided at the national and supranational levels (and stand the test of legality under Union law), EU and Member State initiatives directed at enabling law enforcement access to electronic information held by private companies across borders must plan for the involvement of *effective oversight mechanisms* (Carrera and Stefan, 2018, pp. 13-18). These mechanisms are in particular necessary to monitor that the gathering of data is consistent with the national and EU fundamental rights and rule of law standards that apply to criminal investigations, and access to data in this specific context.

Against this backdrop, independent judicial scrutiny over the issuing *and* execution of requests for data emerges as essential. The involvement of independent judicial authorities is first of all

¹⁹ Opinion 1/15, notably para. 141.

²⁰ Other rights potentially impacted by LEAs' cross-border access to electronic information include the right to non-discrimination (Article 21 EU Charter), freedom of movement (Article 45 EU Charter), freedom of expression (Article 11 EU Charter), and freedom of assembly and of association (Article 12 EU Charter). See Galli (2018).

required to verify that data located across the border are requested by prosecuting authorities and disclosed by companies in a lawful way, this being a precondition for electronic information to be admitted as evidence in court (Carrera and Mitsilegas, 2017). Furthermore, the judicial assessment of requests issued by foreign authorities is also necessary to ascertain that, in the extraterritorial exercise of their criminal jurisdiction, the latter remain bound to EU primary and secondary law, and respect national constitutional and criminal law applying to the collection and processing of data for criminal justice purposes.

When undertaken before the disclosure of the data sought for criminal investigations, independent judicial oversight increases legal certainty and avoids the conflict of laws that typically arises when multiple jurisdictions governed by different constitutional and criminal law traditions (e.g. adversarial or inquisitorial) are involved in transnational law enforcement actions. In substance, the judicialisation of supranational and international cooperation on evidence gathering helps to maintain trust among the parties concerned in a cross-border criminal proceeding (both intra-EU and with third countries).

Contrary to what happens in the context of police or internal security activities, cross-border access to data conducted through *judicial* cooperation in criminal matters is designed to ensure the reliability and accuracy of the information requested, accessed and shared, as well as the lawfulness of the proceedings.

2.2. The role of independent judicial scrutiny in cross-border criminal proceedings

Within the AFSJ, cross-border cooperation in criminal matters is firmly based on the principle of mutual recognition of judicial decisions between Member States' authorities. Judiciaries of the Member States are requested to execute each other's decisions based on the assumption that they fully comply with the EU's foundational principles, as provided under Article 2 of the Treaty on European Union (TEU) and corresponding international obligations (Bárd, 2018).

The mutual recognition principle is based on the presumption that all EU countries' legal and institutional systems provide sufficient fundamental rights and rule of law safeguards. Such a presumption is generally referred to as *mutual trust* (Van Ballegooij, 2015, p. 354). Ascription of judicial authorities as the depositary of trust in EU criminal matters ultimately depends on the division of powers principle,²¹ which presumes their structural independence in assessing whether the execution of another Member State's order will not infringe EU principles, laws and values.²²

²¹ See European Commission for Democracy through Law (Venice Commission) (2016), p. 21, para. 74.

²² According to the definition provided by the European Commission, the principles upon which the EU rule of law concept rests include legality, which implies a transparent, accountable, democratic and pluralistic process for enacting laws; legal certainty; prohibition of arbitrariness of the executive powers; independent and impartial courts; effective judicial review including respect for fundamental rights; and equality before the law. See European Commission (2014), p. 4.

Mutual trust is in fact not unconditional, as confirmed by the automatic execution of cross-border judicial decisions under the mutual recognition principle being subject to exceptions and derogations. These exceptions can be activated when a judicial authority in the country required to recognise another Member State's criminal law measure (including cross-border investigative measures and data-gathering requests) finds that its execution would expose the concerned individual to a risk of a violation of the fundamental rights and rule of law standards provided under EU law.

This 'rebutability' of the mutual trust principle has been repeatedly affirmed in a number of judgments in which the CJEU has had to assess the extent to which the fundamental rights of criminal suspects should be taken into account by the national court executing another Member State's law enforcement measure. In its landmark decision in the joint *Aranyosi and Căldăraru* cases, the Court stressed that judicial scrutiny in the executing country is needed to adequately test and ascertain human rights compliance on the ground, and on the basis of concrete evidence. In fact, executing authorities have the responsibility to postpone, and eventually refuse, the execution of another EU country decision if there are "substantial grounds" to believe that the individual concerned would be exposed to a real risk of inhuman or degrading treatment, within the meaning of Article 4 of the Charter.²³

The Court established a "two-step procedure" to be applied by an executing judicial authority in order to assess the existence of a ground justifying exceptions to the operationalisation of the principle of mutual recognition in criminal matters. That authority must, first of all, make a finding of general or systemic deficiencies in the protections provided in the issuing Member State and, then, seek all necessary supplementary information from the issuing Member State's judicial authority as to the protections for the individual concerned. If the existence of a real risk cannot be discounted within a reasonable time, the Court concluded that the executing judicial authority must decide whether the cross-border procedure should be brought to an end.²⁴

Most recently, the Court has confirmed that mutual recognition in criminal matters should be halted, by way of exception, when the executing judicial authority has objective, reliable, specific and properly updated material²⁵ indicating that systemic or generalised deficiencies affecting the independence of the issuing Member State's judiciary expose the suspect's right to a fair trial to a real risk. In fact, "the high level of trust" on which judicial cooperation in criminal matters is based relies on the premise that the criminal courts of Member States meet the requirement of effective judicial protection which include, in particular, the independence

²³ Joined Cases C-404/15 and C-659/15 PPU *Aranyosi and Căldăraru*, Judgment of 5 April 2016 [ECLI:EU:C:2016:198], para. 104.

²⁴ *Ibid.*, para. 104.

²⁵ Such as that set out in a reasoned proposal of the European Commission adopted pursuant to Article 7(1) TEU. See Case C-216/18 PPU *Minister for Justice and Equality v LM (Deficiencies in the system of justice)*, Judgment of 25 July 2018 [ECLI:EU:C:2018:586], para. 79.

and impartiality of those courts.²⁶ At the basis of the CJEU decision in Case C-216/18 PPU *LM*, is the consideration that judicial independence is an essential corollary of the effective judicial protection principle (Article 19 TEU) and a requirement stemming from the right to an effective remedy before a tribunal (Article 47 EU Charter). In substance, the CJEU confirmed that it is the responsibility of national courts to halt or suspend judicial cooperation if doubts arise as to respect for the rule of law in the issuing state (Van Ballegooij and Bárd, 2018).

Judicial scrutiny by executing Member State authorities is therefore crucial, especially in a context where the Member States' criminal justice systems perform differently under important judicial independence indicators.²⁷ At the EU level, these indicators include factors such as the procedures for the appointment or dismissal of judges, as well as the organisation and functioning of prosecution services.²⁸ The reasoned proposal submitted by the Commission to activate the Article 7 TEU mechanism, and the two infringement procedures based on Article 258 TFEU launched in response to the Polish legislative measures adopted for judiciaries²⁹ prove that restrictions imposed upon judicial independence in one Member State have far-reaching consequences for other countries of the Union.

National courts are to ensure “the full application of European Union law (...) and (...) judicial protection of an individual’s rights under that law”.³⁰ The case law of the Luxembourg Court shows that this responsibility relies upon both the judicial authority issuing or validating a decision to enforce criminal jurisdiction across borders, and the courts of the EU country where such a cross-border law enforcement measure is to be executed. However, systemic dysfunctions arise when one of the two parties involved in cross-border judicial cooperation no longer operates under the rule of law, and notably does not meet the *minimum standards of independence* from the executive that are needed to safeguard the persons concerned in a criminal proceeding.³¹

The CJEU has provided important clarifications in respect of who qualifies as an independent judge under EU law. The Court has stressed that the term ‘judicial authority’ can refer to Member States’ judges, courts and national authorities required to participate in administering criminal justice.³² This definition does not encompass administrative authorities such as

²⁶ Ibid., para. 58.

²⁷ As shown in the 2018 EU Justice Scoreboard, in some EU Member States the executive has a “strong influence” on the appointment and dismissal of court presidents. See European Commission (2018f), pp. 41-44.

²⁸ At the EU level, assessment of the independence of Member States’ judges and prosecutors is conducted in light of the standards elaborated by the Council of Europe. See, in particular, Recommendation CM/Rec(2010)12 of the Council of Europe Council of Ministers to Member States on judges and Recommendation Rec(2000)19 on the role of the public prosecution in the criminal justice system, adopted by the Committee of Ministers of the Council of Europe in October 2000, paras 4, 11, 13 and 34.

²⁹ The two infringement procedures concern the Polish law on the ordinary courts organisation (C-192/18) and the Polish law on the Supreme Court. See European Commission (2018d).

³⁰ See Opinion 1/09 of the Court (Full Court), 8 March 2011 [ECLI:EU:C:2011:123].

³¹ See United Nations Office of the High Commissioner for Human Rights (2018).

³² In Cases C-452/16 PPU *Poltorak* of 10 November 2016 [ECLI:EU:C:2016:858], C-477/16 PPU *Kovalkovas* of 10 November 2016 [ECLI:EU:C:2016:861], and C-453/16 PPU *Özcelik* [ECLI:EU:C:2016:860], of 10 November 2016.

ministries or police authorities, which are “within the province of the executive”.³³ Such an exclusion is justified in light of the need to respect the rule of law and the principle of separation of powers on the one hand, and the need to uphold mutual trust stemming from the judicialisation of cooperation on the other (Carrera and Mitsilegas, 2018).

The Court has recently highlighted the importance of judicial independence in the EU legal system. This emerges from the CJEU’s decision in the case *Associação Sindical dos Juizes Portugueses* of 28 February 2018,³⁴ which dealt with the legality of a reduction in the remuneration of public officials and judges in Portugal due to its interference with the principle of judicial independence. In this ruling, the Court also provided the first interpretation of Article 47 of the EU Charter, and specifically of the right to an effective remedy and fair trial:

The principle of the *effective judicial protection* of individuals’ rights under EU law, referred to in the second subparagraph of Article 19(1) TEU, is a general principle of EU law stemming from the constitutional traditions common to the Member States, which has been enshrined in Articles 6 and 13 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950, and which is now reaffirmed by Article 47 of the Charter.

The ruling goes on to state that

the very existence of effective judicial review designed to ensure compliance with EU law is of the essence of the rule of law.³⁵

In this decision, the Court also provided a clear set of conceptual features determining the extent to which a judicial authority is ‘independent’ for the purposes of EU law, by stating “the factors to be taken into account in assessing whether a body is a ‘court or tribunal’ include, inter alia, whether the body is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is *inter partes*, whether it applies rules of law and whether it is independent”.³⁶

In this same ruling, the CJEU confirmed that “ensuring judicial review in the EU legal order” is not only “a responsibility of the Court of Justice but also [of] national courts and tribunals”. Article 19(1) TEU states that “Member States shall provide remedies sufficient to ensure effective legal protection in the fields covered by Union law” (emphasis added), which include criminal justice and the gathering of evidence in this domain. By specifying effective judicial protection as a general principle of EU law, and defining who qualifies as an independent judicial authority in EU law, the Court set important benchmarks for testing the legality of EU and international policy initiatives to introduce criminal law instruments allowing unmediated access to electronic data (Carrera and Mitsilegas, 2018).

³³ Ibid., para. 35.

³⁴ Case C-64/16 [ECLI:EU:C:2018:117].

³⁵ Ibid., paras. 35 and 36 (emphasis added).

³⁶ Ibid., para. 38.

The CJEU has in fact clearly established as a criterion to determine compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the EU Charter of Fundamental Rights the need to make access by the competent national authorities to communications data dependent on a prior review carried out by a court or by an independent administrative body, whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued, and which intervenes following a *reasoned request* of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions.³⁷ Thus, the access to such data by competent national authorities shall only be regarded as constituting a lawful limitation of the EU fundamental rights to the right to respect for private life, and of the right to the protection of personal data, if carried out after such prior independent scrutiny.

The prior review by a court or independent administrative body is essential to ensure respect of the principle according to which access to data needs always to be limited to what is strictly necessary, based on objective criteria defining the circumstances and conditions of such access.³⁸ When based on laws allowing to grant access to data with the objective of fighting serious crime, access should be granted only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime.³⁹ In particular situations, for example concerning vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted, but only if there is objective evidence from which it can be deduced that the data might, in a specific case, make an *effective contribution* to combating such activities.⁴⁰

The European Court of Human Rights (ECtHR) also recently determined that in an EU Member State (the United Kingdom) the acquisition by a public authority of communications data from a communications services provider required that data access be subject to prior review by a court or independent administrative body.⁴¹ Otherwise, the requirement derived from its own case law regarding the need for any interference with the rights of Article 8 of the European Convention on Human Rights (ECHR) to be “in accordance with the law” could not be regarded as fulfilled. The ECtHR reached such conclusion by taking into account already referred CJEU case law.⁴²

Additionally, the ECtHR stressed that the lack of prior review by a court or independent administrative body in every case where there is a request for the communications data of a journalist, or where such collateral intrusion is likely, must be regarded as a violation of the

³⁷ *Digital Rights Ireland*, para. 62.

³⁸ *Tele2 Sverige AB*, para. 118.

³⁹ *Ibid.*, para. 119.

⁴⁰ *Idem.*

⁴¹ Judgment of the Court (First Section) of 13 September 2018, *Case of Big Brother Watch and Others v the United Kingdom* [ECLI:CE:ECHR:2018:0913JUD005817013]; see especially paras. 463, 466 and 467.

⁴² In particular the *Digital Rights Ireland* judgment.

rights recognised in Article 10 of the ECHR,⁴³ on the right to freedom of expression and information.

Provided that important differences exist among Member States in terms of administrative bodies that qualify as independent (Mitsilegas and Vavoula, 2018), the question arises as to how to ensure EU fundamental rights and rule of law standards – and specially to satisfy the effective judicial protection requirement – when the requesting country gathers data directly from the private company holding or controlling it. By granting LEAs the power to obtain data directly from private companies, initiatives such as the CLOUD Act and the Commission’s proposal for Production and Preservation Orders aim at equipping LEAs with new tools that will speed up the gathering of data located outside their country’s territory.

Nevertheless, to qualify as judicial cooperation in criminal matters, the cross-border gathering of electronic data cannot fall short of systematically ensuring that independent judicial scrutiny is carried out in *both* the country issuing the request (or order) and the country where the data are stored, and *before* the access to data is granted. Ensuring that the persons concerned by cross-border requests for access to data are covered by the guarantees provided under EU law becomes challenging in the absence of independent scrutiny by judicial authorities in the requested state to validate the lawfulness of accessing and processing data.

3. EU secondary law on cross-border evidence gathering for criminal justice purposes

The EU has engaged in extensive internal and external action in the fields of criminal justice and data protection, and over time has developed a normative framework for judicial cooperation governing the gathering and exchange of evidence in the context of cross-border criminal proceedings taking place within the EU or at the international level.

MLATs (signed respectively with the US and Japan) and the EIO enable the transmission of requests (and responses to requests) for electronic information sought in the framework of a domestic criminal investigation, but held across borders. Both the MLATs and the EIO adopt a model of formal judicial cooperation designed to ensure that cross-border requests for data respect the sovereignty of the foreign country on whose territory an investigative measure needs to be implemented.⁴⁴

Most notably, EU Member States have the responsibility to ensure that foreign cross-border transfers of data falling under EU jurisdiction are compatible with the fundamental rights and rule of law standards provided in the EU legal system. These standards must be adhered to by all Member States as well as private companies addressed by third countries’ authorities seeking EU data, regardless of factors such as the nationality of the data subject or the place of establishment of the service provider holding the data sought. The lack of a direct ‘interest’ in

⁴³ Ibid., paras. 496-499.

⁴⁴ European Commission (2018a), p. 22.

the criminal prosecution of the Member State where the company is located (or legally represented) cannot exempt the authorities of that country from their *obligation* to verify that foreign requests for data are processed in compliance with both domestic and EU rules.

3.1. Mutual legal assistance and the EU legal framework for transatlantic data transfer in criminal proceedings

MLATs, which are the traditional channel of cooperation for cross-border gathering and exchange of electronic information, are currently used by EU Member States in cases where cross-border criminal proceedings concern a Member State that does not participate in the EIO Directive, such as Denmark and Ireland. Available MLA instruments for intra-EU cooperation include the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters and its Protocols ('1959 MLA Convention'), the Convention Implementing the Schengen Agreement and the 2000 Convention on Mutual Legal Assistance in Criminal Matters between the Member States ('2000 EU MLA Convention') and its Protocol.

As for relations with third countries, more specifically transatlantic cooperation, the already mentioned EU–US MLA Agreement complements existing bilateral treaties and amends some of their provisions, if they provide for less effective avenues of cooperation between EU Member States and the US.⁴⁵ As submitted by the Commission, the Agreement “largely relies on existing and future bilateral agreements with particular [Member States]”.⁴⁶ If the Agreement supplements existing bilateral agreements, “the latter do not operate in isolation from Union Law”.⁴⁷ For Member States that do not yet have an agreement with the US, the EU–US MLAT may provide a suitable legal basis for cooperation. The standards set by the EU–US Agreement are also “a benchmark” for the conclusion of future bilateral agreements in the field between Member States and the US.⁴⁸

Exchange of evidence under MLATs relies on the involvement of different authorities, including the political bodies and judicial actors responsible for supervising and examining cross-border requests for evidence gathering against domestic standards. The exact ways in which MLA requests are issued and processed largely depends on the specific constitutional tradition and relevant legal framework of the countries concerned (Carrera et al., 2015, pp. 7-8). Despite respecting national specificities, a consistent feature of the MLA process is the mediation by the competent national authorities required to ensure that the cross-border request for access to electronic information is in line with the legal and procedural requirements of the requested country.

⁴⁵ See Article 3(2)(a) of the EU–US MLA Agreement.

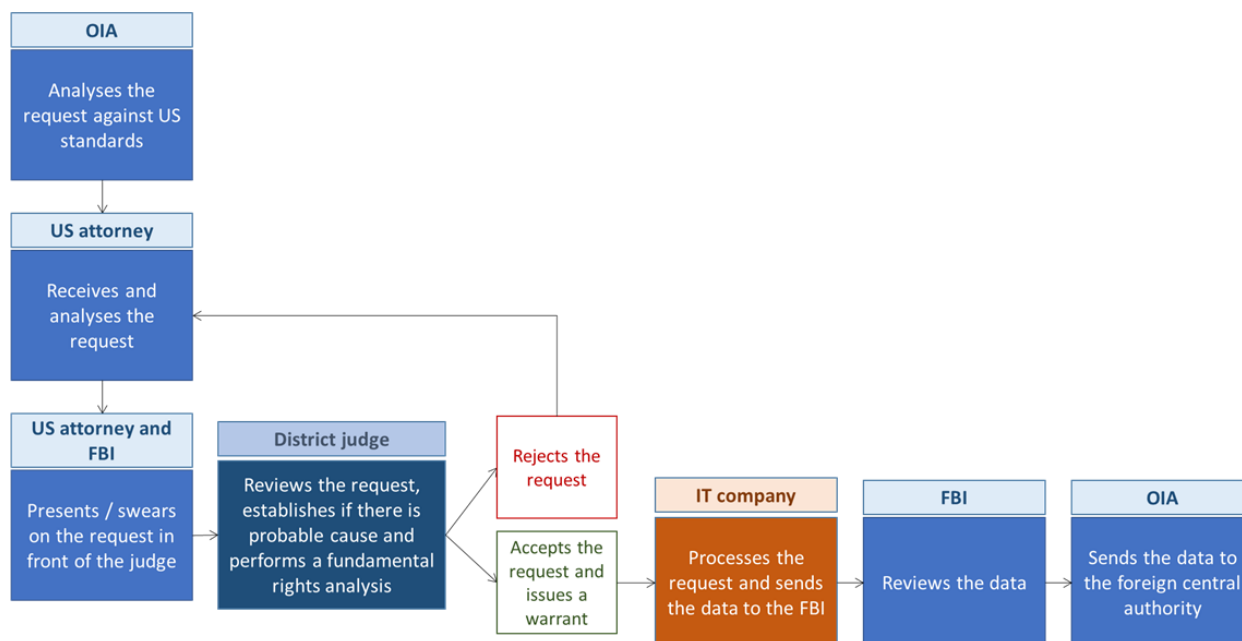
⁴⁶ European Commission (2018a), p. 23.

⁴⁷ Council of the European Union (2016a), p. 3.

⁴⁸ Ibid.

Figure 1 provides a schematic description of the different steps and authorities involved in the processing of an MLA request issued by EU Member State authorities for obtaining electronic data in the US.

Figure 1. US processing of EU Member State MLA requests for data



Note: OIA = Office for International Affairs.

Source: Authors' own elaboration.

EU law enforcement requests for access to data stored in the US are assessed against the probable cause standard under the Fourth Amendment⁴⁹ and specific provisions of statutes, such as the Electronic Communications Privacy Act (ECPA), which protects wire, oral and electronic communications in transit.

The Stored Communications Act (SCA), which is contained in Title II of the ECPA, is a blocking statute that limits the possibility for foreign governments to directly request content data held by IT companies in the US, by subjecting their possibility to access electronic information to the requirement of independent judicial validation. While foreign LEAs can directly ask IT companies to disclose non-content data (which respond on a voluntary basis), the content of

⁴⁹ The Fourth Amendment limits the government's ability to conduct searches and seizures, and warrants can be issued only with independent review by a judge. The Fourth Amendment governs more than simply a person's home or body; its protections apply specifically to communications, covering a person's "papers and effects". Probable cause that a crime has been committed must be established by the law enforcement officer by "reasonably trustworthy information" that is sufficient to cause a reasonably prudent person to believe that an offence has been or is being committed or that evidence will be found in the place that is to be searched.

electronic communications might only be produced when a US federal judge has been satisfied of the existence of “probable cause”.⁵⁰

For certain categories of information, the ECPA would require less than probable cause. For instance, the statute specifies that data or electronic communications that have been in storage for more than 180 days can be produced upon the issue of a subpoena or a court order, which occurs when a judge is persuaded of the existence of ‘specific and articulable facts’ enabling the assumption that the requested data are relevant to an ongoing criminal investigation. Still, federal appellate courts have progressively extended application of the probable cause requirement to these requests.⁵¹ In any case, LEAs cannot be exempted from the obligation to obtain an independent judge’s authorisation to access content data stored in the US.

Under the MLA process, in substance, the foreign case is subject to the same standards and protections as a national case. The same principle should also apply to US requests for data held in the EU. Nevertheless, the practice adopted by US authorities has consistently been to bypass MLA channels to request data held by US companies abroad, including in the EU. In these cases, US authorities follow the same domestic process as if the data were located in the US.⁵² Following this approach, an MLA request would only be issued if the data were held abroad by a non-US company. This US practice of bypassing MLA channels might contribute to explaining the imbalance in numbers of outgoing and incoming requests under the EU–US MLA Agreement. Estimations made in the context of the 2016 EU–US MLA Review exercise revealed a 4:1 ratio of requests to the US compared with requests coming from the US.

The legality of the US authorities’ practice to order private companies to disclose data stored in the EU has been challenged in the already mentioned *Microsoft Ireland* case. The dispute essentially questioned the lawfulness of extraterritorial assertion of US criminal jurisdiction in light of standing (i.e. pre-CLOUD Act) domestic legislation. The US Department of Justice argued that its warrant authority under the SCA required US-based companies to turn over the requested data, regardless of where the latter were stored. Microsoft, by contrast, defended that this authority did not extend to data located outside United States territory.

The question, however, was far from being an exclusively domestic one. Foreign authorities’ unmediated (extra-MLA) access to data stored in the EU raises far-reaching issues also from the EU law perspective. As already observed, the risk of a conflict of laws, or, more directly, of violation of EU standards, emerges if foreign investigators’ requests for electronic data falling

⁵⁰ LEAs must prove that an offence has been or is being committed or that evidence will be found in the place that is to be searched.

⁵¹ In the *United States v Warshak* case (2010), the Sixth Circuit broadened the interpretation of the Fourth Amendment’s guarantees expanding the probable cause standard also to communication that has been in storage for more than 180 days. In *Riley v California* (2014), the Supreme Court stated that “the police generally may not, without a warrant, search digital information on a mobile phone seized from an individual who has been arrested”. In the *Carpenter v United States* case (2018), the Supreme Court ruled that in order to obtain mobile phone tracking information (metadata/non-content), law enforcement authorities needed a warrant.

⁵² In addition, the ‘Bank of Nova Scotia’ doctrine allows for subpoenas (instead of search warrants) to be sent to a US-based company to produce evidence stored outside the US. See Kyriakides (2014).

under EU jurisdiction are not assessed in light of the rule of law guarantees and fundamental freedoms (encompassing both criminal justice and privacy-related rights) provided under EU primary and secondary law; in particular, if personal data affected by subsequent data transfers do not benefit from a level of protection ‘essentially equivalent’ to the protection granted under EU law.⁵³ EU fundamental rights safeguards are binding upon EU Member States as well as foreign countries and private companies, and are granted to everyone regardless of nationality.

With the introduction of the CLOUD Act, the US intended to establish a (US and international) legal and operational framework for LEAs across the Atlantic to obtain data directly from companies abroad. Part I of the Act⁵⁴ formally grants US LEAs the power to order private companies to disclose the “content of a wire or electronic communication and any record of other information” about a person, regardless of either the nationality of the latter or the location of the data. Providers can also be ordered to preserve data in their possession for up to 180 days prior to the issuance of any compulsory process. Part II of the CLOUD Act,⁵⁵ on the other hand, enables the conclusion of “executive agreements” between the US government and “qualifying foreign powers”. These agreements will allow non-US governments to directly request the data of non-US persons from US-based companies without going through the MLA process. These requests would be compulsory upon the companies *based on the law of the issuing country*.

From an EU law perspective, a number of questions arise with regard to the CLOUD Act’s fitness to provide a sound legal basis for the gathering and transfer of data in the context of cross-border criminal proceedings. Article 48 of the General Data Protection Regulation (GDPR)⁵⁶ states:

Any 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 recognised 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.⁵⁷

What Part I of the CLOUD Act appears to authorise, instead, is the transfer of personal data falling under EU jurisdiction exclusively upon the order of US authorities, meaning outside any EU international agreement or legally binding instrument in force between the parties.

⁵³ Schrems, para. 73.

⁵⁴ Section 103 of the CLOUD Act.

⁵⁵ Ibid., Section 105.

⁵⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council 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).

⁵⁷ Article 48 of Regulation (EU) 2016/679 (emphasis added).

In its *amicus curiae* brief submitted on behalf of the EU to the Supreme Court in the *Microsoft Ireland* case,⁵⁸ the European Commission recognised that a company might have a “legitimate interest” in complying with a foreign authority’s order to transfer data sought in the framework of a criminal investigation. A refusal to comply with the order could, in fact, lead the company to be subject to a legal action in a non-EU state (i.e. the US). That notwithstanding, the Commission also made clear that EU law only allows such transfers where the company’s legitimate interest is not “overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data”.⁵⁹ The reason for having EU rules on transfers of personal data to a non-EU state is precisely to avoid that – in the extraterritorial application of their domestic law – foreign authorities hamper the attainment of the protection that in the Union is provided to all natural persons.

It is true that Article 49 of the GDPR provides for the possibility to *derogate* from MLA processes. However, this norm does not seem to provide an appropriate EU legal basis to justify all transfers of data ordered by the US under the CLOUD Act. Under this specific GDPR provision, data transfers are permissible “only if the transfer is not repetitive”, if it “concerns only a limited number of data subjects” and only if “the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data”. Article 49 explicitly concerns “derogations for specific situations”, and must be interpreted strictly. Under the CLOUD Act, US authorities are instead given unlimited jurisdiction over any data (including content, metadata and subscriber information) controlled by US companies abroad.

With regard to CLOUD Act provisions related to the executive agreements to be concluded between the US and “qualifying foreign governments”, doubts emerge as to the possibility for EU Member States to act bilaterally in a field where the Union has legislated extensively, both internally and externally. The Commission has already noted that bilateral agreements with non-EU countries would lead to “fragmentation” of the EU legal framework regulating access to data for law enforcement purposes.⁶⁰ As recent research has shown, EU Member States are pre-empted from the conclusion of an international agreement with third countries on the exchange of personal data for law enforcement purposes, at least to the extent that such an agreement would undermine EU fundamental rights and rule of law standards (Carrera, et al., 2018, p. 43). It is noteworthy that when the CLOUD Act was passed, the European Commissioner for Justice and Consumers Věra Jourova stressed that the measure “narrows the room for potential compatible solutions” between the EU and the US (Jourova, 2018).

A fundamental problem of compatibility with EU law arises also with regard to the disparity in the guarantees that under any given CLOUD Act executive agreement would be granted, on the one hand, to “United States persons” and, on the other hand, to persons from the rest of the world – including EU citizens. In fact, the CLOUD Act establishes that US constitutional

⁵⁸ See European Commission (2017a).

⁵⁹ Ibid., p. 9.

⁶⁰ European Commission (2018a), p. 78.

safeguards would continue to apply only to foreign requests for data targeting US citizens or aliens lawfully admitted (for permanent residence) to the country. No specific guarantee is provided by the CLOUD Act as to the level of protection granted to EU citizens' data in the US, especially in the case where an executive agreement is signed between the US and a non-EU country.

Safeguarding EU citizens against the risks that derive from divergences in the level and scope of fundamental rights protection granted respectively by the EU and the US legal systems has been a key point of controversy in previous transatlantic discussions on international data transfers, which eventually led to the adoption of the EU–US Umbrella Agreement.⁶¹ The main objective underlying the EU–US Umbrella Agreement is precisely to ensure adherence to EU data protection standards in transatlantic data transfers. These standards apply when personal data are exchanged for reasons relating to the prevention, investigation, detection and prosecution of criminal offences, and also cover transfer by private companies in the territory of one party to the competent authority of the other party. The Umbrella Agreement grants EU citizens the possibility to seek judicial remedies before US courts if US authorities mishandle their data.

However, the EU–US Umbrella Agreement “in and of itself shall not be the legal basis for any transfers of personal information”, as it rather represents a “framework” for the protection of personal data that are exchanged between the US and EU Member States. In transatlantic relations, the basis for the exchange of evidence in criminal law matters is instead provided by the EU–US MLA Agreement.⁶² The latter provides for “collection of evidence by consent”, and is designed to embody “a carefully negotiated balance” between not only the interests, but also the obligations of different states.

According to current criticisms, the most prominent practical issue that affects the EU–US MLA Agreement lies in the delays that are experienced in the execution of MLA requests (Daskal, 2016). If smoothing cooperation under the EU–US MLA Agreement is essential to improve the fight against crime, previous research has shown how some of the delays faced by competent authorities in the attempt to obtain electronic information through the implementation of MLA procedures could be addressed through practical measures. These include for example the deployment of specialised personnel (e.g. national contact points and liaison magistrates) to promote reciprocal understanding of the legal systems involved and smooth cooperation among the different jurisdictions concerned; the streamlining of processes for requesting and providing assistance; and the allocation of sufficient financial and human resources to appropriately follow up the MLA requests.

⁶¹ Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, OJ L 336/3, 10.12.2016.

⁶² Agreement of 25 June 2003 on mutual legal assistance between the European Union and the United States of America, OJ L 181, 19.7.2003, pp. 34-42.

To stand the test of legality under EU law, any further initiative between the EU and the US would need to take into account the benchmarks of judicial cooperation provided under the MLA system. Exercising reciprocal judicial scrutiny over incoming LEA requests for data emerges in particular as an essential requirement under EU law.

On the one hand, such scrutiny enables the protection of the subject whose data fall under EU law, as confirmed by the fact that under the EU–US MLA Agreement requests issued by US authorities directed at obtaining data stored in the EU by non-US companies have been refused on grounds such as the absence of dual criminality, a failure to demonstrate a nexus between the evidence sought and the criminal conducted alleged, and on the basis of essential interests.⁶³ On the other hand, it serves the purpose of ensuring that EU citizens’ fundamental rights are appropriately guaranteed in the US.

3.2. The European Investigation Order

May 2017 marked the entry into force of the Directive on the European Investigation Order in criminal matters. The proposal for the directive was tabled in April 2010 by a group of eight Member States.⁶⁴ Except for Denmark⁶⁵ and Ireland,⁶⁶ all the EU Member States currently participate in the EIO Directive. All participating EU countries have by now transposed this piece of EU law in their national legislation, although in some cases (e.g. Austria, Luxembourg and Spain) transposition only occurred in the second half of 2018.⁶⁷

Even before transposition, the EIO was already considered ‘inefficient’. In this regard, it is interesting to note that a joint Europol and Eurojust paper presented to the Council in March 2017 anticipated that “the EIO framework may not accommodate (...) the speed that is required to capture electronic evidence. Moreover, the Directive does not contain provisions that specifically facilitate the collection of common types of electronic evidence, meaning that additional tools need to be developed to facilitate the collection of electronic evidence under the EIO framework.”⁶⁸ If it is true that EIO legislation does not expressly mention “electronic evidence” as such, Article 13 of the EIO Directive nonetheless refers to ‘data’. This indicates that evidence may indeed be gathered and exchanged in electronic form through the EIO. At the same time, and similar to MLAs, the EIO set forth standards that must be met if *electronic data* collected as part of a criminal investigation are to qualify as *evidence* accepted as ‘admissible’ before a court of law.

⁶³ Council of the European Union (2016a).

⁶⁴ These were Austria, Belgium, Bulgaria, Estonia, Luxembourg, Slovenia, Spain and Sweden.

⁶⁵ Denmark exercised a general opt-out from all EU justice and home affairs measures – see Protocol 22 attached to the Treaties.

⁶⁶ Ireland still has the possibility to opt into the EIO Directive by virtue of Protocol 21 attached to the Treaties.

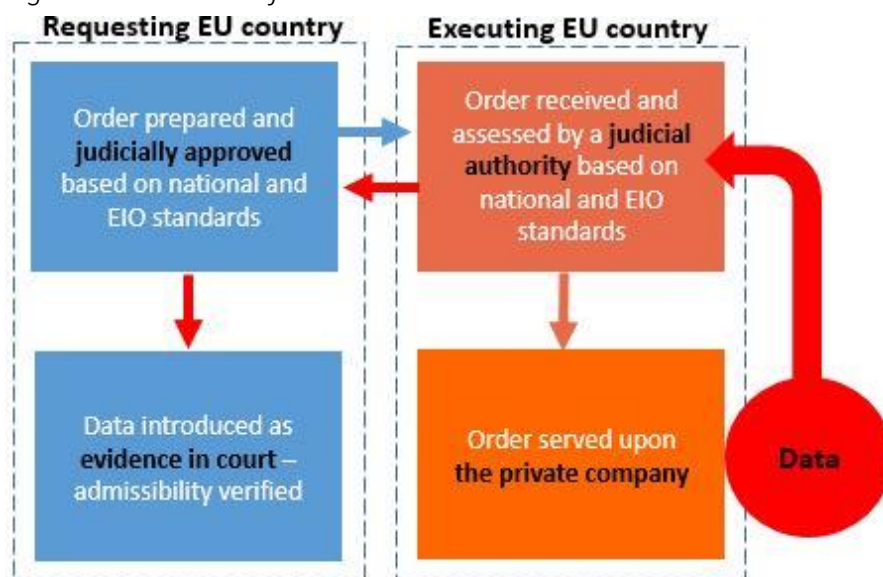
⁶⁷ European Judicial Network (2018).

⁶⁸ See Eurojust and Europol (2017).

The EIO Directive creates a “single, efficient and flexible instrument”⁶⁹ to be used for the execution of cross-border investigative measures, including those involving the gathering of electronic data in the territory of other Member States. This new tool replaces previous instruments for criminal justice cooperation regulating the exchange of evidence through mutual legal assistance. It aims at reducing the uncertainty related to the fragmentation of the pre-existing framework of cooperation.⁷⁰ Outside the EIO, EU Member States’ formal cooperation for the gathering of information (including electronic data) in the framework of criminal proceedings is still governed through MLATs. The EIO Directive foresees that Member States may conclude or continue to apply bilateral or multilateral agreements or arrangements with other Member States only to the extent that these “make it possible to strengthen the aims” of the EIO.⁷¹ These aims consist of simplifying and facilitating the procedures for gathering evidence in full compliance with EU law safeguards.

The EIO Directive responded, in the first place, to the goal of facilitating cross-border criminal investigations by extending the principle of mutual recognition to the field of evidence gathering in criminal proceedings. In practice, the EIO consists of a judicial decision that a competent authority of a Member State issues or validates in order to have one or several specific investigative measures carried out in another Member State (see Figure 2).

Figure 2. Execution of an EIO



Sources: Authors’ elaboration.

⁶⁹ Council of the European Union (2016b), p. 2.

⁷⁰ The framework included the 1959 Council of Europe Convention, ratified by all of the EU Member States; the Benelux Treaty of 1962; the Convention for the application of the Schengen agreements of 1990; the Convention Implementing the Schengen Agreement; and the 2000 EU MLA Convention, with its Protocol of 2001. Some provisions related to the gathering of evidence for criminal proceedings were also introduced through the Framework Decisions 2003/577/JHA on freezing property or evidence and 2008/978/JHA on a European Evidence Warrant.

⁷¹ Article 34(3) of the EIO Directive.

The instrument was chiefly designed to speed up the procedure for transmitting requests involving investigative actions across borders and to reduce the possible grounds of refusal by limiting the degree of discretion that, under the MLA system, is left to the authorities required to execute foreign investigative measures (Bachmaier Winter, 2010).

The EIO Directive exempts the executing authority from assessing double criminality, as it provides for the execution of the EIO *if* it relates to an offence that is punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years and falls within one of the 32 categories of offences listed in Annex D of the Directive.⁷² The EIO should be executed within the strict time limits provided in the Directive.⁷³ In this regard, the Directive specifies that the competent authorities of the Member State receiving an EIO will have a maximum period of 30 days to decide to recognise and execute the request, and 90 days to execute the request effectively. The Directive also allows for a shorter deadline when required by the seriousness of the offence or in other particularly urgent circumstances, and this should be taken into account as much as possible when processing the order.⁷⁴ Article 32(2) of the Directive provides for a 24-hour deadline for provisional measures, such as the preservation of data. This provision can thus be used in urgent cases. Furthermore, the executing authorities should take a final decision on the execution of the EIO and carry out the required investigative measure(s) with the “same celerity and priority as for a similar domestic case”.⁷⁵

The EIO Directive contributes to enhancing judicial cooperation in the field of evidence gathering also by providing for the execution of a wide range of investigative measures. EIOs are not limited to the preservation (freezing) phase, and go beyond the objective of preventing the destruction, transformation, movement, transfer or disposal of existing evidence. In fact, the Directive allows Member States to issue an order for the executing country to conduct new investigative measures directed at *obtaining and transferring* information – including electronic data – previously unavailable to the competent authorities, with minimum formality.⁷⁶ Such investigative measures might also cover the “collection of traffic and location data associated with telecommunications, allowing competent authorities to issue an EIO for the purpose of obtaining less intrusive data on telecommunications”.⁷⁷

Besides introducing a demand-based system for conducting cross-border investigative measures based on swift procedures and minimum formalities, the EIO also sets

⁷² Article 11(1)(g) of the EIO Directive. This list replicates Article 2(2) of the Framework Decision on the European Arrest Warrant. There is no express political offence exception; however, see recital 39.

⁷³ Article 12(3)–(5) of the EIO Directive).

⁷⁴ Ibid., Article 12(2-4).

⁷⁵ Ibid., Article 12(1).

⁷⁶ By contrast, a freezing order issued under Framework Decision 2003/577/JHA on freezing property or evidence was required to be accompanied by a separate request for the transfer of evidence to the state issuing the order in accordance with the rules applicable to mutual assistance in criminal proceedings.

⁷⁷ Recital 11 of the EIO Directive.

unprecedented ‘benchmarks’ for EU judicial cooperation in criminal matters with the objective of guaranteeing a set of supranational safeguards in complying with the legal and constitutional system of the executing Member State (Carrera et al., 2016).

In the first place, the issuing of an EIO is only possible in relation to acts or facts that are punishable under the national law of the issuing country,⁷⁸ and when the judicial decision of the issuing Member State may give rise to proceedings before a court having jurisdiction in criminal matters.⁷⁹ These provisions aim at preventing Member States from employing the EIO to obtain evidence abroad that they are not able to obtain under their own domestic legal and constitutional procedures, and at ensuring that these cross-border investigative measures are not used for police-to-police cooperation per se. The deployment of the EIO is specifically directed at the collection of information related to facts that constitute a criminal offence worthy of review in a judicial proceeding.

Judicial authorities are centrally involved during both the issuing and executing phases of the EIO. The EIO Directive clearly stipulates that *any decision* to issue an EIO taken by an authority other than a judge, court, investigating magistrate or public prosecutor must be validated by one of those bodies (Glaser et al., 2010). Furthermore, the executing authority must comply with the formalities and procedures expressly indicated by the issuing authority only to the extent that these are not contrary to the fundamental principles of law of the executing state. This assessment entails judicial scrutiny by the competent authority of the executing state with regard to the legality, necessity and proportionality of the investigative measures requested through the EIO.

This judicial scrutiny might lead the executing authority to refuse to recognise and execute an EIO, for instance for certain categories of (less serious) offences for which the requirement of dual criminality has not been met, or when the execution of the investigative measure requested under the EIO would not be authorised under the law of the executing state in a similar domestic case (Heard and Mansell, 2014). Consistent with this proportionality requirement, the EIO Directive allows the executing authority to 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 than the investigative measure indicated in the EIO”.⁸⁰ In substance, the EIO Directive aims at increasing mutual trust and cooperation between competent judicial authorities of EU Member States, while at the same time preserving the specificities of the national systems and their legal culture.

⁷⁸ See Article 6(1)(b) of the EIO Directive. This provision has been included to avoid instances where Member States use the EIO to ‘fish’ for evidence.

⁷⁹ Article 4 of the EIO Directive.

⁸⁰ Article 10(3) of the EIO Directive.

This piece of EU legislation also requires judicial authorities to verify whether the execution of an EIO is compliant with fundamental rights standards.⁸¹ The EIO Directive reiterates the limits to the mutual recognition principle in the preamble:

if there are substantial grounds for believing that the execution of an investigative measure indicated in the EIO would result in a breach of a fundamental right of the person concerned, and that the executing State would disregard its obligations concerning the protection of fundamental rights recognised in the Charter, the execution of the EIO should be refused.⁸²

Judicial actors are called upon to verify whether specific grounds of legitimate refusal to recognise and execute an EIO exist. These grounds are quite specific and include cases where the execution of an EIO could lead to a breach of rules on immunity or privilege, or rules limiting criminal liability relating to freedom of the press, or where it could harm essential national security interests, or infringe the *ne bis in idem* principle.⁸³ The wording of the Directive seems to suggest that a defect in this regard by another Member State should be judged in *individual* cases (De Capitani and Peers, 2014). National legal traditions are also safeguarded by provisions establishing that the executing authorities may refuse the execution of an EIO when “the use of the investigative measure indicated in the EIO is restricted under the law of the executing state to a list or category of offences or to offences punishable by a certain threshold, which does not include the offence covered by the EIO”.⁸⁴

In cases where a claim is made that the issuance or execution of an EIO would lead to a breach of individual rights, the EIO Directive requires that “remedies equivalent to those available in a similar domestic case” are made available against the investigative measures adopted under the EIO.⁸⁵ It also includes provisions ensuring that information about remedies is provided, that time limits for doing so are reasonable and that the rights of the defence are considered. However, challenges to the substantive reasons for issuing an EIO are solely possible before the authorities of the issuing country (Heard and Mansell, 2014).

In addition, the EIO Directive provides that the suspected or accused person, or the lawyer on his/her behalf, may require the issuing of an EIO, “within the framework of applicable rights of the defence in conformity with national criminal procedure”.⁸⁶ Moreover, the defendant can be confident that, once the foreign authorities will have received the EIO, they will be under considerable pressure to execute it, as it is an order coming from another EU judicial authority rather than an ordinary MLA request (Carrera et al., 2018, p. 80). Once the EIO is executed, the

⁸¹ Ibid., Article 11(1)(f).

⁸² Ibid., Recital 19.

⁸³ Ibid., Article 11.

⁸⁴ Ibid., Article 11(1)(h).

⁸⁵ Ibid., Article 14.

⁸⁶ Ibid., Article 1(3).

executing authority should, without undue delay, transfer the evidence obtained or already in its possession to the issuing state.

Finally, the Directive makes explicit reference to the first three post-Lisbon measures dealing with procedural guarantees for criminal suspects, namely: Directive 2010/64/EU on the right to interpretation and translation in criminal proceedings; Directive 2012/13/EU on the right to information in criminal proceedings; and Directive 2013/48/EU on the right of access to a lawyer and the right to communicate when deprived of liberty. These references can be read as a requirement to interpret and implement the post-Lisbon EU criminal justice *acquis* in a consistent manner.

4. The European Commission's e-evidence proposals

In April 2018, the European Commission tabled two legislative proposals on the gathering of electronic evidence in criminal matters. Both proposals respond to the goal of equipping LEAs with binding instruments that, if adopted, could be used to directly address private companies across borders and compel them to secure and provide electronic information sought for a criminal proceeding.

The first is a proposal for a regulation foreseeing the introduction of two new crime-fighting tools, namely the European Production and Preservation Orders. The European Production Order consists of a mandatory request that Member State LEAs could issue to obtain a piece of electronic information directly from a company in another Member State. The European Preservation Order would instead impose upon service providers outside the issuing Member State the obligation to preserve stored data in view of a subsequent request to produce such data. The subsequent request to obtain the preserved data could originate from the Member State issuing the Preservation Order, but also from another Member State conducting a criminal investigation or a third country.

The second consists of a proposal for a directive that would introduce an obligation for private companies – including communications service providers, social networks, online marketplaces and all providers of internet infrastructures (e.g. internet protocol (IP) addresses and domain name registries) – in the EU to appoint at least one legal representative to act as a point of contact for Production and Preservation Orders addressed by LEAs.

The proposal covers companies and service providers operating in one or more Member States, wherever their headquarters are located or the information sought is stored. The legal representative would be responsible – on behalf of the company – for “receiving, complying with and enforcing”⁸⁷ the European Production and Preservation Orders proposed under the new e-evidence regulation. As shown in Table 1, the personal scope of the Commission's proposals is broader than that of the CLOUD Act, which only concerns US companies.

⁸⁷ See European Commission (2018d), p. 4.

Table 1. Personal scope (e-evidence proposals and the CLOUD Act)

Service providers concerned	
E-evidence proposals	CLOUD Act
<p>All digital service providers, including</p> <ul style="list-style-type: none"> • electronic communications (covering telecommunication) service providers; • information society service providers; and • providers of internet infrastructure services and marketplaces. <p>They fall under the scope of the e-evidence proposals as long as they offer services in the EU market, even if</p> <ul style="list-style-type: none"> • the <i>data are stored abroad</i> (e.g. in the US); • the main site of the company is <i>not established in the EU</i>; and • the <i>service is provided from abroad</i>. 	<p>US companies, including</p> <ul style="list-style-type: none"> • electronic communications service providers (such as email providers); and • remote computing service providers (including certain cloud storage providers). <p>They fall under the scope of the CLOUD Act if their main site is in the US, when:</p> <ul style="list-style-type: none"> • the data (including contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within the provider's possession) is <i>stored in the US</i>; • the data are <i>stored abroad</i> (e.g. in the EU).

Note: The indicators used to ascertain whether a service is provided in the EU market include availability of the service in an EU Member State language that is not widely spoken outside the EU and the possibility to pay in euros. The mere accessibility of the service from the EU is not considered sufficient.

Sources: Authors' elaboration based on European Commission (2018a), p. 52, and CLOUD Act, Sec. 103, para. 2713.

In terms of material scope, the scope of the Commission's proposals encompasses different categories of electronic information, mainly distinguished between content data (e.g. text, voice, videos, images and sounds stored in a digital format) and non-content data (including subscriber data, metadata, access logs and transaction logs).⁸⁸

4.1. Background of the proposals

As requests to access and gather electronic information have become a common criminal investigative practice at the national, regional and international levels, policy and legislative efforts have increasingly sought to find alternatives to both the system of voluntary nature of current service provider's cooperation with LEAs, and the 'mediated' model of cross-border cooperation for access to data provided by the EIO and MLATs.

At the EU level, discussions on the need to create a tool facilitating access to electronic data for cross-border criminal proceedings started in 2015 when the Commission presented the

⁸⁸ See the glossary in this report.

European Agenda on Security⁸⁹ and they advanced in parallel with other (different) initiatives put forward under the so-called Security Union strategy.⁹⁰ The European Council and the Council of the European Union have been particularly supportive of the Commission's work to facilitate the gathering of electronic data sought by Member State authorities involved in criminal proceedings. In its Conclusions on "improving criminal justice in cyberspace", adopted in June 2016, the Council stressed the need for EU action in this respect.⁹¹

Based on consultations with stakeholders conducted as part of the expert process launched after the June 2016 Council Conclusions, the Commission presented a non-paper that identified several options for improving access to electronic information for crime-fighting purposes.⁹² These options varied in nature and objectives, and aimed at tackling issues related to the different instruments available for investigating and prosecuting authorities to obtain data from service providers, both within the EU and in cooperation with the US.

A first set of options consisted of "practical measures" to improve cooperation among law enforcement and judicial actors, and their interactions with companies holding the data.⁹³ These consisted of non-legislative actions relying on the framework of cooperation already provided under the existing EU and international legal instruments (i.e. the EIO and MLATs). They included the idea to create an electronic (and user-friendly) version of the EIO, and the establishment of a platform (using the e-CODEX system) for fostering digital exchanges and replies between EU judicial authorities. Among the considered measures there was also the possibility to create single points of contact to ease and streamline cooperation between public authorities and service providers. According to the Commission, these measures could *address inefficiencies in public-private cooperation*, specifically by reducing delays in responses.⁹⁴

Other solutions proposed consisted of soft-law measures aimed at improving cooperation between Member States and US judicial and diplomatic authorities through the organisation of technical dialogues, training, and exchange of information and best practices on applicable rules and procedures related to the issuing and treatment of MLA requests in a transatlantic context. As for direct cooperation with service providers for access to non-content data, the main suggestions for improvement consisted of streamlining companies' policies and practices, as well as the standardisation and reduction of forms used in Member States to facilitate the creation of "quality requests".⁹⁵

While acknowledging the potential of these practical measures to improve cooperation among judicial authorities and between the latter and private companies, the Justice and Home Affairs

⁸⁹ The document stressed the need for eliminating any "obstacles to criminal investigation of cybercrime", including those deriving from existing rules on access to electronic data. See European Commission (2015).

⁹⁰ See European Commission (2018e).

⁹¹ Council of the European Union (2016b).

⁹² European Commission (2017b).

⁹³ Ibid., p. 2.

⁹⁴ European Commission (2018a), p. 46.

⁹⁵ Ibid., p. 47.

Council of June 2017 highlighted how a “large majority” of Member State ministers supported the need to consider EU legislative action to enable LEAs to access data through direct cooperation with service providers.⁹⁶ As noted in the report on the outcome of the Justice and Home Affairs Council meeting of June 2017, in view of the “sense of urgency” raised by a number of ministers with regard to EU legislative action on “e-evidence”, the Commission announced its intention to present a legislative proposal in early 2018.⁹⁷

4.2. The e-evidence proposals in light of EU primary and secondary law standards

4.2.1. *The right legal basis? Criminal justice vs police cooperation*

The impact assessment accompanying the e-evidence proposals qualifies the European Production and Preservation Orders as judicial cooperation instruments designed to bring into being a “new dimension in mutual recognition”. Consequently, the Commission has chosen Article 82 TFEU as a legal basis for the proposed regulation on European Production and Preservation Orders for electronic evidence in criminal matters.

The argument advanced to justify the Commission’s choice of this specific legal basis is that Article 82(1)(d) TFEU envisages the possibility to adopt criminal justice measures directed not only at “facilitating” cooperation between judicial or equivalent authorities of the Member States, but also at “enforcing” decisions taken by these authorities in relation to proceedings in criminal matters (Ligeti and Robinson, 2017, p. 111). Yet, it seems questionable that the execution of a Member State authority’s decision to access personal data by a private company can be qualified as judicial cooperation, especially in a context where the role left to judicial authorities in the operationalisation of the proposed instruments remains overall limited.

According to the Commission’s proposal, judicial authorisation in the issuing country would be required, but only when a Production Order concerns the production or preservation of specific types of (i.e. transactional or content) data. Judicial scrutiny would not be required as far as non-content data, and notably subscriber and access data, are concerned. Indeed, it is proposed that disclosure of the latter types of information could be ordered directly by prosecutors.⁹⁸ The same applies to European Preservation Orders which, it seems, could also be issued by a prosecutor (i.e. without independent judicial validation), and regardless of the types of data concerned.⁹⁹ Nor does the proposed regulation foresee the systematic involvement of the competent judicial authorities of the Member State where the data, or the

⁹⁶ Many ministers, however, underlined that in developing such a framework, due account must be taken of the issues of data protection.

⁹⁷ Council of the European Union (2017).

⁹⁸ See Article 4 of the proposed Regulation; see also the proposed Regulation Explanatory Memorandum, p. 16.

⁹⁹ As indicated by the Commission in the proposed Regulation Explanatory Memorandum, “to enable investigating authorities to act fast and given that the relevant request to produce the data will be the subsequent request where all the conditions will again be scrutinised, European Preservation Orders may also be issued or validated by a prosecutor”, p. 17.

company holding it, are located. Judicial actors of this EU country would only *eventually* and *accidentally* be involved in the process, in cases where the *service providers* decide not to execute the order served upon them based on pre-defined grounds of “non-compliance” (see Figure 3 below).

The Commission claims that the ‘orders’ would introduce a ‘new model’ of direct private–public cooperation in criminal matters that ‘builds upon’ the principle of mutual recognition.¹⁰⁰ This interpretation appears difficult to square with the scope of Article 82(1) TFEU as well as of Article 67(3) TFEU, which circumscribe the application of mutual recognition instruments to cooperation between competent Member State authorities. In fact, it is among the latter that a relationship based on reciprocal trust is established under EU law – there is no general assumption of reciprocal trust between public authorities and private companies. Under existing mutual recognition instruments decisions need to come from a judicial (or equivalent) authority in the issuing state and their execution *requires the prior involvement of a judicial authority* in the Member State where the addressee or the object concerned by the measure is located.

The question seems very much one of checks and balances within the EU criminal justice system. EU primary law calls for the prosecutor’s actions affecting fundamental rights (like the search of personal information) to remain under the control of independent judges. In the Explanatory Memorandum to the e-evidence proposal the Commission recognises that the use of the proposed instruments could potentially affect a number of fundamental rights, including the right to protection of personal data, the right to respect of private and family life, the right to freedom of expression, the right of defence, the right to an effective remedy and to a fair trial. However, the proposed regulation offers no guarantees that independent judicial scrutiny will be ensured automatically and systematically in the issuing country, nor in the country where the addressee is located.

In light of the consolidated CJEU jurisprudence on the operationalisation of the mutual recognition principle in criminal matters, it cannot be assumed that the prior involvement of a judicial authority in the Member State issuing the orders alone is sufficient to ensure that the person concerned by a criminal measure is not exposed to the risks of fundamental rights violations (see section 2.2. above). As noted by the Council of Europe’s Venice Commission, in some countries “a ‘*prosecutorial bias*’ seems to lead to a quasi-automatic approval of all such requests from the prosecutors. This is a danger not only for the human rights of the persons concerned but for the independence of the judiciary as a whole.”¹⁰¹ Nevertheless, under the proposed regulation the judicial authorities of the state to which the order is addressed would have no opportunity to make their own assessment when the service providers directly comply with a European Production or Preservation Order issued by another EU country (see subsection 4.2.3 below).

¹⁰⁰ European Commission (2018a).

¹⁰¹ European Commission for Democracy through Law (Venice Commission) (2011), p. 14 (emphasis added).

Rather than facilitating the mutual recognition of judicial decisions within the Union, the proposed regulation appears to mainly be directed at enabling law enforcement actors, and in particular police and prosecutors, to request, access, collect and share data held by companies across borders and sought during the pre-trial or trial phase of a criminal proceeding. The achievement of this goal will depend on the establishment of a framework of cooperation under which service providers receive, assess and respond directly to a foreign law enforcement order to produce or preserve data. Based on the above, it is worth asking whether Article 82(2)(a) TFEU (police cooperation among the Member States in criminal matters) would better reflect both the main *aim* and *content* of the e-evidence proposals.

In this regard, it is important to remember that under EU law the choice of legal basis for any EU action must be supported by objective factors, “amenable to judicial review”.¹⁰² The distinction operated in the EU Treaties between judicial cooperation in criminal matters (where independent judges are central figures and monitor trust), and police cooperation (where LEAs, including prosecutors, carry out law enforcement investigations for the purpose of fighting crime) is central in this respect, and must be reflected in the legal basis selected for specific EU instruments.

As clearly stressed by the CJEU, “if an examination of an act of the Union reveals that it pursues a *twofold aim*, or that it has a twofold component, and if one of those is identifiable as the main one, and the other is *merely incidental*, the measure must be based on a single legal basis, namely that required by the *main aim* or component”.¹⁰³ In any case, when an EU measure “simultaneously pursues a number of objectives or has *several components* that are indissociably linked, without one being secondary and indirect in relation to the other, such an act will have to be founded on the *various corresponding legal bases*”.¹⁰⁴

It is also concerning to note that any reference to Article 16(2) TFEU (respect of personal data) is currently missing from the Commission’s proposals. Any EU measure seeking to counter terrorism and crime must in fact go hand in hand with data protection safeguards. As a consequence, it appears that an instrument aimed at enabling data collection in a law enforcement context cannot but also encompass this EU primary law provision. In its recent Opinion on the proposals on European Production and Preservation Orders for electronic evidence in criminal matters, the European Data Protection Board also has questioned the Commission’s choice of legal Basis (EDPB 2018, p. 4).

Doubts have also been expressed with regard to whether the selected legal basis suffices to adopt Article 13 of the draft regulation, which obliges the Member States to provide for pecuniary sanctions for violations of the obligations under Articles 9–11. The potential

¹⁰² Opinion 1/15, para. 55.

¹⁰³ Case C-178/03 *Commission of the European Communities v European Parliament and Council of the European Union* [ECLI:EU:C:2006:4], para. 42 (emphasis added).

¹⁰⁴ *Ibid.*, para. 43 (emphasis added).

harmonising effect of this provision on the substantive criminal laws of the Member States may require an additional legal basis (Meijers Committee, 2018).

4.2.2. *Concerns over necessity, legality and proportionality*

The proposed regulation is said to have a limited scope.¹⁰⁵ In that regard, its draft Article 5 proposes to only allow the issuing of European Production Orders for transactional and content data when the underlying offence is capable of attracting a custodial sentence of three years or more, or when the underlying offence falls under one of the definitions adopted under EU instruments regarding money counterfeiting, child sexual abuse, cybercrime and terrorism. By contrast, Production Orders targeting subscriber data and access data may be issued for any criminal offence.¹⁰⁶ A series of doubts arise with regard to the compatibility of these provisions with the principles of necessity, legality and proportionality.

In the first place, limiting the application of a European Production Order to criminal offences punishable by custodial sentences of at least three years can hardly be qualified as a real limitation. Under the penal codes of the Member States, a very large number of offences fall under this category, including offences that are not considered to constitute a serious crime. In this regard, it is important to recall that other international cooperation mechanisms (e.g. the UN) set higher thresholds.

Furthermore, Article 5 refers to definitions of crime adopted at the EU level in areas in which Member States are allowed to provide for broader definitions of crime at the national level. In any case, to date the concept of “serious crime” has not been defined by EU law, and the circumstances that allow law enforcement actors to order service providers to produce data still depend on specific national legislation and vary by Member State.¹⁰⁷

Somehow contradicting the view according to which the scope of the proposed regulation is limited, the Commission has stressed that the initiative is not limited to serious crime, as “the problem of cross-border access to e-evidence in criminal investigations is relevant for all crimes”.¹⁰⁸ The absence of a precise vision and definition of which crimes are actually covered by the proposal is particularly problematic, especially in a context where there is no involvement of a second-line check of legality, necessity and proportionality by judicial authorities in the Member State where the order is addressed.

The CJEU has traditionally limited the possibility to retain and collect both traffic and location data for law enforcement purposes when this is necessary for the prosecution of individuals suspected of having committed a serious crime. In the *Ministerio Fiscal* judgment, the CJEU recognised that legitimate derogations to the principle of confidentiality of electronic

¹⁰⁵ See pp. 5-6 of the draft regulation Explanatory Memorandum

¹⁰⁶ Article 5(3) of the proposed Regulation.

¹⁰⁷ Case C-207/16 *Ministerio Fiscal* [ECLI:EU:C:2018:788], para. 95 and following.

¹⁰⁸ See European Commission (2018a), p. 44.

communications are not strictly limited to the fight against serious crime, but can be admitted also, if they constitute non-serious interferences,¹⁰⁹ when it is necessary for the investigation and prosecution of other (non-serious) ‘criminal offences’. The case, nevertheless, did not concern a request to access traffic and location data but only the phone numbers linked to specific SIM cards, and data about the identity of their owners, during a very limited period of time.

In any case, the Court also restated in that judgment that access by public authorities to personal data retained by service providers constitutes an interference with the fundamental rights of privacy and data protection, without it being relevant that the information in question is sensitive or whether the persons concerned have been inconvenienced in any way. In substance, data accesses that are necessary for the fight against non-serious crime must also always be proportionate in light of their impact on fundamental rights provided under the EU Charter.

Ensuring the proportionality of data gathering in criminal prosecution under the new regulation would become particularly difficult also because independent judicial validation is not systematically guaranteed in the issuing country, nor in the country where an order is to be executed, for all instances of data transfer. Judicial scrutiny is not required as far as the production of non-content data, and notably subscriber and access data, are concerned. It is in fact proposed that disclosure of the latter types of information can be ordered directly by prosecutors.¹¹⁰ Moreover, orders to produce those types of personal information can be issued for any criminal offence. European Preservation Orders can also be issued without independent judicial validation, and regardless of the type of data concerned.

Table 2. Standards applying to the issuing of Production Orders

Type of data	Threshold	Issuing authority
Subscriber data	Any criminal offence	Judicial authority or prosecutor
Access data	Any criminal offence	Judicial authority or prosecutor
Transactional	Offences carrying a maximum custodial sentence of 3 years or more (or catalogued offences)	Judicial authority
Content	Offences carrying a maximum custodial sentence of 3 years or more (or catalogued offences)	Judicial authority

Source: Authors’ elaboration based on the proposed Regulation.

¹⁰⁹ *Ministerio Fiscal*, para. 61.

¹¹⁰ See Article 4 of the proposed regulation; see also the proposed regulation Explanatory Memorandum, p. 16.

At the same time, as the impact assessment to the Commission proposal shows, most of the cross-border requests for access to data are currently directed at obtaining non-content information.¹¹¹ If passed in its current form, the Commission proposal could lead to an unprecedented increase in volumes of data requests in criminal investigations. The European Commission states that investigators seek electronic evidence in “around 85% of criminal investigations”, and that over half of those law enforcement investigations “involve a cross-border request to access electronic evidence”.

The risk is legalising ‘fishing expeditions’ whereby investigators order service providers to produce or preserve large troves of non-content data in the hope that the information they receive will bear out assumptions made during early stages of the criminal investigations, and simultaneously collect data which are not directly related to the criminal offence for which the investigative measure was adopted. Without judicial validation by an independent judge, it will become extremely difficult to ensure that the requested information is restricted to what is relevant and necessary for the prosecution of a crime. Additionally, the proposal in its current shape does not foresee a general obligation for public authorities issuing the order to reimburse the service providers for the cost incurred in executing the order. Such a provision could potentially act as a deterrent to avoid the automatic issuing of orders in all criminal investigations. However, the proposed regulation leaves it to the single Member State to decide whether (and in which cases) to refund service providers for the costs incurred in processing the orders.

When used to obtain content data, the new instruments could mean increasing the administrative burden in national judicial systems, with judges being potentially exposed to a large number of ‘orders’ to be reviewed. Furthermore, it is not clear how the high volumes of ‘raw’ data obtained will be dealt with, or to what extent they will actually be admitted as ‘evidence’ in criminal proceedings. In fact, the proposed regulation establishes that data should be provided regardless of whether the service provider is able to decrypt the information or disclose it in an encrypted form only. It is not clear whether the authorities receiving the encrypted data will have the necessary technical capacity and resources to make them usable for the scope of the proceedings. Still, to ensure the necessity and proportionality of the proposal it is necessary to assess precisely in which cases the execution of a Production Order would lead to the collection of data that can produce probatory material before a criminal court. There is a risk that the data collected will never be presented in court, upon which shall thus not be fully entrusted the judicial review of the measures at stake.

Under existing mutual recognition instruments, and namely the EIO, the scrutiny conducted by judicial authorities in the phase that precedes the execution of cross-border criminal justice measures also serves the purpose of ensuring that immunities and privileges protecting the data sought in the Member States of the company are adequately taken into account. Under the proposed regulation, it would instead be for the authorities of the issuing state to verify the

¹¹¹ See European Commission (2018a), p. 14.

existence of potential immunities or privileges.¹¹² This would not be an easy task, as it would presume that the issuing authorities possess an in-depth knowledge of specific provisions related to accessing electronic data for criminal justice purposes, as regulated in the other 26 Member States' legal systems.

4.2.3. Issues arising from the execution, review and enforcement of the proposed orders

In the Commission's proposals, the exclusion of the execution state's judicial authorities during the phase that precedes the actual execution of the order is to be compensated by the involvement of the private companies (or their legal representatives) upon which such a measure is served.¹¹³ It would thus become the latter's responsibility to verify the subsistence of grounds justifying the refusal to execute a Production or Preservation Order. This new role that the draft regulation assigns to private companies is highly problematic, for a number of reasons.

The proposal seems to impose upon private companies a general obligation to comply with the certificate transmitting the orders (i.e. the European Production Certificate (EPOC), or the European Preservation Order Certificate (EPOC-PR)).¹¹⁴ This is confirmed by the introduction of financial penalties, especially foreseen to incentivise companies to produce or preserve the data sought by prosecuting authorities in cross-border criminal investigations.¹¹⁵ True, the proposed regulation also allows service providers to object to the automatic execution of the proposed orders. However, the only legitimate grounds for raising exceptions are substantially limited to cases where the certificate transmitting the order is incomplete, manifestly incorrect or the data requested have been (lawfully) deleted or are not in the possession of the addressees.¹¹⁶ Outside these cases, any ISP or company refusal to execute the order is automatically considered a case of "non-compliance".

¹¹² Article 5 of the proposed Regulation.

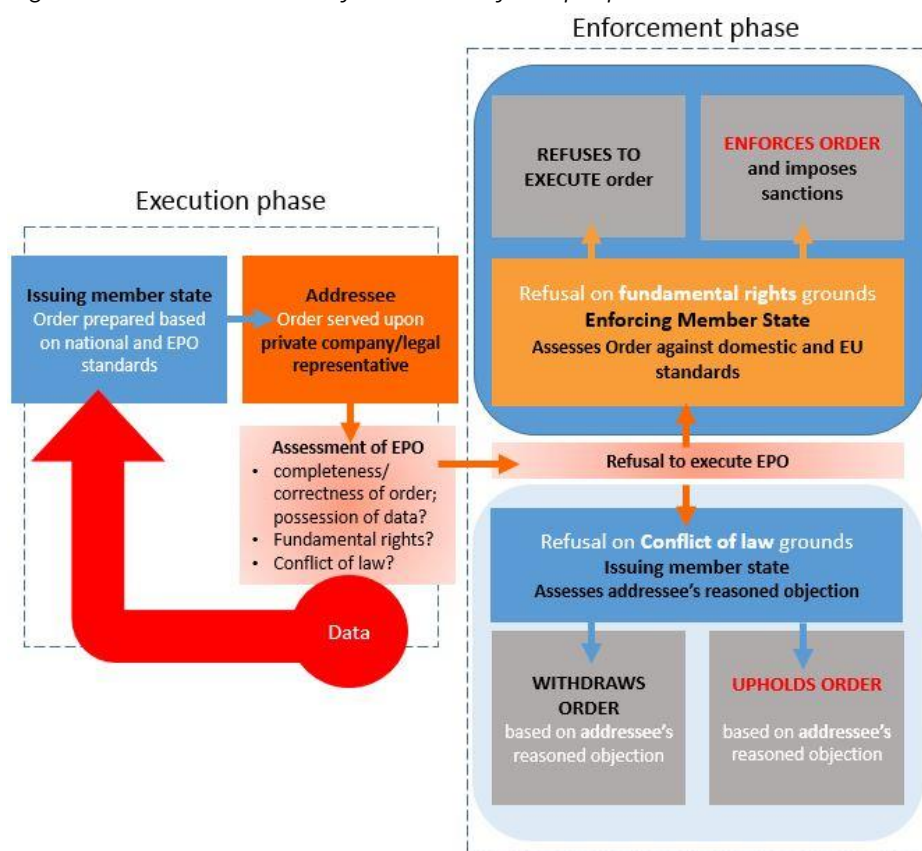
¹¹³ Ibid., Article 7.

¹¹⁴ Ibid., Articles 9 and 10.

¹¹⁵ Ibid., Article 13.

¹¹⁶ Ibid., Article 9.

Figure 3. Execution and enforcement of the proposed orders



Note: EPO = European Production/Preservation Order.

Source: Authors elaboration

For each case (or hypothesis) of non-compliance contemplated by the proposed regulation, a specific type of enforcement procedure would follow, as shown in Figure 3 above.

Non-compliance based on fundamental rights considerations

The *first hypothesis* of “non-compliance” envisaged by the proposed regulation encompasses situations where the service provider refuses to execute the order because it is “apparent” that granting access to the requested data would result in a “manifest” violation of the EU Charter of fundamental rights, or that the order is “manifestly abusive”. It is important to note these notions do not have definitions in EU law. Fundamental rights risks for the persons concerned by the execution of an order can exist and be relevant even when they are not manifest. The choice to leave private companies with the responsibility to decide when not to execute (and therefore contravene) the order on the basis of vague fundamental rights considerations does not seem to offer the targeted persons (i.e. suspects in criminal investigation, and more in general all the subjects whose data are affected by Production or Preservation Orders) with effective guarantees against potential abuses.

In fact, the decision not to comply can only be based on a *prima facie* fundamental rights assessment to be conducted within a very limited timeframe (ranging from 10 days to a

minimum of 6 hours).¹¹⁷ Furthermore, the proposal does not require the issuing authority to indicate *ex ante* (i.e. in the certificates) important information related to the grounds of necessity and proportionality of the order, nor to include “further details” about the case. The scarcity of information made available constitutes another obstacle to the possibility for the service providers to properly assess the fundamental rights impact of the measure.¹¹⁸

More in general, it appears unrealistic to expect that private companies will effectively engage in this type of sensitive and complex legal assessments, and assume upon themselves the duty to protect fundamental rights. This responsibility is simply not part of the statutory goals of private organisations that pursue exclusively commercial interests. In this regard, it is concerning to note that whereas the proposal sets out financial penalties to ensure service providers comply with the orders served on them, it excludes any responsibility for human rights violations deriving from the production of the data, if the company acted in “good faith”.¹¹⁹ Discharging private companies from human rights responsibilities that might stem from their decision to execute a Production Order appears, however, to be at odds with the principles of corporate social responsibility emerging under international and EU law.¹²⁰

The very rationale underlying the different provisions on the role of service providers does not, as a matter of fact, appear to be concerned with effectively replacing judicial authorities in terms of rule of law requirements, but rather with facilitating their intervention, and mitigating some possible conflicts. If this can be described as concerning a ‘protective function’ (Böse, p. 41), the protection here at stake is not the protection of fundamental rights, but the protection of the interests of service providers – which might of course be legitimate, but are not the only interests endangered by cross-border data access requests.

Non-compliance based on “apparent” lack of judicial validation

The company might also decide not to execute an order when it is “apparent” that judicial scrutiny has not been ensured in the issuing Member State. This is the second hypothesis of non-compliance contemplated by the proposed regulation, which includes the right for the service provider to raise certain claims in the issuing Member State “if the Order has not been issued or validated by a judicial authority”.¹²¹ However, such a ground of refusal to comply can only be raised as far as it relates to orders entailing the production or preservation of content data.¹²² In such cases, the service providers would have the duty to a) verify whether a judge has been involved in the adoption of an order in the issuing country; b) assess whether the involvement of the judicial authority in question offers sufficient guarantees from a

¹¹⁷ See Article 9 of the proposed Regulation. The normal deadline is 10 days, while authorities may set a shorter deadline where justified. Moreover, in emergency cases, defined as a situation where there is an imminent threat to life or physical integrity of a person or to a critical infrastructure, the deadline is 6 hours.

¹¹⁸ Article 5 of the proposed Regulation.

¹¹⁹ Recital 46 of the proposed Regulation.

¹²⁰ See United Nations Human Rights Council (2011).

¹²¹ Proposed regulation Explanatory Memorandum, p. 10.

¹²² Judicial scrutiny is not necessary for other types of data.

fundamental rights and rule of law perspective; and c) decide whether (or not) to object to the execution of the order.

Deliberating upon these issues is very challenging because each Member State provides for a specific method of judicial validation for access to data in the context of criminal proceedings. National legal provisions in this regard differ significantly, with a clear demarcation between adversarial and inquisitorial systems of criminal procedure. In addition, different rules and oversight systems also apply to the issuing of cross-border requests for access to data, depending on the constitutional and institutional framework established in the country concerned. It is unclear how a private company would determine not only who qualifies as an independent judge under national law, but also whether the national judiciaries of various Member States satisfy EU law requirements regarding judicial independence.

Only independent judicial authorities possess the necessary institutional prerogatives and professional capacity to ensure an appropriate assessment of whether a legitimate ground subsists for refusing the execution of another Member State's criminal law enforcement measure. As a consequence, it appears that the new role that the proposed regulation on the European Production and Preservation Orders assigns to service providers risks undermining the coherent application of the effective judicial protection principle enshrined in Article 19 of the EU Charter. This is highly problematic from an EU constitutional law point of view.

Furthermore, the possibility that a company does not object to a request for data where it should do so might also undermine the very objective of the proposed measure. For instance, there is a risk of a service provider or its legal representative executing a Production Order without realising that the targeted data enjoys special protection. In such situations, the result may well be that the data transferred by a service provider to the prosecuting authorities will not be admitted as evidence before a criminal court.¹²³

In the hypotheses on non-compliance described above (i.e. service providers' refusal based on fundamental rights concerns or lack of judicial scrutiny considerations), the order should be enforced by the authorities of the competent Member State where the service provider is established or represented. The "enforcement member state" is responsible for recognising the issuing authorities' order, confirming its enforceability and enforcing it. The fact that the enforcement Member State could well be different from the state where the service is provided, or where the data are located, but, more importantly, where the individuals to whom the data relate are located, adds to the complexity of the procedure.

The draft regulation requires the enforcing authority to recognise and enforce an EPOC or EPOC-PR unless it considers that one of the grounds for refusal applies. These grounds are substantially limited to cases where the enforcing authority ascertains the following:

¹²³ Article 18 of the proposed Regulation.

- the lack of formal judicial authorisation and a substantial threshold (when the orders concern content and transactional data);¹²⁴
- the existence of immunities and privileges, the impossibility of the service providers to comply (*force majeure*), a concern about national security or the European *ordre public*, or manifest violations of fundamental rights that result solely from the information contained in the order;¹²⁵ and
- the outreach of the order beyond the scope of the regulation (when the order is issued outside the pre-trial or trial phase, or when it does not target service providers providing services within the Union).¹²⁶

It is concerning that no further margin of appreciation is left to this eventual ‘executing authority’ as to the assessment of the legality, necessity and proportionality of the orders. At the same time, it is questionable that the authority responsible for the ‘enforcement’ will decide to execute another EU country’s order even when such a measure has not been adopted in accordance with the law of the eventually enforcing Member State.

The notwithstanding, the proposed regulation foresees that the competent authority of the enforcing Member State must enforce the order even if its own domestic law provides for a higher standard of protection than the law of the issuing Member State. For instance, a Dutch authority could be obliged to enforce a Production Order issued by a French authority prosecuting a criminal offence for which, in the Netherlands, a similar measure is not allowed (Böse, 2018, p. 39). Also, and contrary to what is provided for under the EIO Directive, there is no possibility for the eventually enforcing authority to implement the foreign investigative measure through less pervasive means.

Non-compliance based on conflicts of obligations

Companies would be allowed (and thus, presumably expected) to object to the execution of the orders when this is required to solve ‘conflicts of obligations’ between EU law and legal provisions from other jurisdictions (e.g. the US).¹²⁷ This constitutes the *third hypothesis* of non-compliance. These conflicts of obligations are typical of the ‘unmediated model’ for law enforcement access to data and arise when, sometimes 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. The purpose of the Commission’s proposal to compel service providers established outside the Union to appoint legal representatives in the EU is to turn the process of serving a Production Order into an ‘EU internal process’. However, these

¹²⁴ Ibid., Article 14(2), (4)(a–b) and (5)(a).

¹²⁵ Ibid., Article 14(4)(f) and (5)(e).

¹²⁶ Ibid., Article 14(4)(e) and (5)(d).

¹²⁷ Articles 15 and 16 of the proposed Regulation provide for a review procedure if the service providers headquartered in third countries are faced with conflicting obligations.

service providers would remain subject to the legal obligations standing in the (non-EU) foreign legal system where they are established (e.g. the US).

Under the proposed regulation the risks of a conflict of laws are likely to increase not only within the EU, but also when European Production or Preservation Orders are issued for data stored in the US and/or upon US companies. As already noted, the Fourth Amendment requires a warrant with probable cause to provide foreign authorities access to the content of electronic communications stored in the US. It is far from certain that in the absence of such a warrant, service providers will be able to provide EU Member State LEAs access to the requested data without incurring liabilities under US law. Similarly, US authorities' requests for direct access to data held by private companies and falling under EU jurisdiction are likely to raise a conflict of law when disclosure of the requested data would result in a breach of EU primary or secondary law standards protecting fundamental rights, including the EU data protection *acquis*.

The proposed regulation requires the addressee to inform the issuing authority of cases where compliance with the order would cause infringements of the law(s) of a third country. Based on the "reasoned objection"¹²⁸ of the service provider, the issuing authority may choose whether to withdraw the order or to uphold it.

In the latter option, the case would be transferred to the competent court of the issuing Member State. It would therefore be up to the authorities of the latter to decide not only if the law of the third country applies to the case and if a conflict of law actually exists, but also to assess the lawfulness of the foreign legislation protecting the data against access. In carrying out the assessment, the issuing Member State court would have to decide whether the law of a third country is intended to protect legitimate interests (e.g. fundamental rights, or national security) or instead to shield illegal activities from LEA requests to data access.

The proposed regulation requires the issuing Member State's court that "ascertain[s]" the existence of a conflict of jurisdiction to request the "central authorities" of the third country concerned to express their opinion over the conflicting obligations. Yet, it is not clear whom, in the foreign jurisdiction, would ultimately be responsible to address the conflict of laws (Meijers Committee, 2018).

If a conflict of law is found to exist (e.g. in the eventuality that the data request by the EU authority is directed at a company subject to US jurisdiction), the authority seeking the data will have to go through the MLA process. In these cases, the time required to execute the investigative measure originally provided for in the order would be longer than the one typically required to request and obtain data across borders directly through existing MLA channels.

¹²⁸ See in particular Articles 15(1), 16(1) and 2(1) of the proposed Regulation.

4.2.4. Effectiveness and accessibility of remedies under the European Production and Preservation Order proposals

As seen above, the proposed regulation includes a set of provisions aimed at granting service providers and individuals the possibility to challenge Production and Preservation Orders. At the same time, the actual availability, accessibility and effectiveness of the different complaint mechanisms that the Commission's proposal foresees vary significantly.

As already noted, service providers are granted a (limited) possibility to contravene an EPOC or EPOC-PR served upon them. If deciding not to execute the order, the addressee has the right to be heard before the authorities of the enforcement countries (the first and second hypotheses of non-compliance) or by the authorities of the issuing country (the third hypothesis of non-compliance).

Nevertheless, the right of a non-compliant service provider to obtain an *effective judicial remedy against a sanction would be undermined* by the limited possibility that the eventually involved authority would have to refuse the recognition and enforcement of the order. As noted above, the authorities eventually involved in the enforcement phase might decide not to enforce the order only in specifically circumscribed circumstances (*force majeure*, the European *ordre public*, manifest fundamental rights abuses, etc.). A negative assessment of the legality, necessity and proportionality of the issuing authority's order is not included among the grounds that could be used to oppose its enforcement.

Another point of concern relates to the prospect that individuals may lack clear indications as to exactly which country and authority to bring their claims that rights or procedural rules are violated in the issuing or execution of a European Production Order. Article 17 of the draft regulation provides that both the suspect of a crime concerned by a European Production Order and persons whose data were requested without them being suspect or accused in criminal proceedings could seek remedies in the country of the issuing authority. The suspect and accused person or third parties whose data have been transmitted would have the right to challenge the legality of the order according to the law of the issuing Member State.¹²⁹

At the same time, it is very likely that a situation will arise in which the individual involved – either being a suspect or not – resides in a Member State that is different from both the issuing Member State and the state on which territory the company's legal representative or establishment is placed (Meijers Committee, 2018, p. 4). The risk is increasing uncertainty for affected individuals as to which country is responsible for assessing the complaint. This risk escalates in cases where service providers are requested by the issuing authorities to ensure the confidentiality of the EPOC or the EPOC-PR and of the data produced or preserved.¹³⁰

Challenges to adequately assess complaints by affected individuals would also arise in cases where the courts in the issuing state are in fact not the 'best placed' to satisfy the requirements

¹²⁹ Article 17(1) and (3) of the proposed Regulation.

¹³⁰ Article 11(2) of the proposed Regulation.

of impartiality and independence necessary to ensure an effective and practical safeguarding of the right of access to justice. In view of that, it must be considered less obvious to only allow individuals to lodge their complaint in either the issuing Member State or the state in whose territory a company preserved or transmitted the requested data. Doubts exist as to the actual possibility for individuals to bring their complaints before an independent court in their state of residence.

4.2.5. EU privacy and data protection safeguards

The proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters also raises a number of important data protection issues.

The two most significant issues regarding data protection concern, first, the very necessity of the measures foreseen by the proposal, and second, its systematic reliance on the idea that some categories of data might be processed subject to only a very limited set of legal requirements, on the basis of the alleged *relatively limited* impact on fundamental rights of their processing.

The first question is linked to the justification for publishing the proposal. As detailed in the Explanatory Memorandum accompanying the text, the European Commission's main argument in this respect is that the current situation is problematically fragmented and characterised by legal uncertainty; the existing landscape, indeed, would be the result of juxtaposing "mechanisms for cooperation between countries [that] were developed several decades ago"¹³¹ and a series of "national tools" developed since by some Member States and third countries.¹³²

The proposal, however, would not replace existing mechanisms and tools,¹³³ but rather offer an additional possible path to access data. Although it might actually reduce legal certainty for companies potentially subject to conflicting obligations,¹³⁴ it does not, as such, reduce legal uncertainty for individuals – on the contrary, it adds an extra layer of unpredictability. As a result of the proposal, it would become even more difficult than currently for individuals to be able to determine who has access to their personal data, and on which grounds (which are dependent on the jurisdiction of the issuing authority, possibly not their own). Today's fragmented and complex¹³⁵ reality would thus not be improved. Instead, the proposal could be interpreted as enabling data processing in an unforeseeable manner, which would be in direct tension with EU fundamental rights requirements.

¹³¹ See the proposed Regulation Explanatory Memorandum, p. 1.

¹³² Idem; also echoed in recital 8 of the proposed Regulation.

¹³³ See for instance, "[t]his instrument will co-exist with the current judicial cooperation instruments that are still relevant and can be used as appropriate by the competent authorities" (ibid., p. 2); and "[t]he new instrument will not replace the EIO for obtaining electronic evidence but provides an additional tool for authorities" (ibid., p. 3).

¹³⁴ Illustrating the focus on service providers' perspectives is recital 9 of the proposed Regulation.

¹³⁵ Ibid., p. 7.

A second critical issue refers to the idea according to which it is justified to attach (and, more critically, de-tach) different conditions to the processing of the various categories of data put forward in the proposal on the grounds of their “different levels of interference with fundamental rights”.¹³⁶

In this context, it must be noted that EU data protection law generally applies to any processing of personal data, exclusively because they are personal data in the sense of related to an identified or identifiable person. Although it is true that some special types of personal data (falling under the notion of ‘sensitive’ data) are granted special, additional protection, and that certain types of processing are regarded as involving a higher risk and thus subject to added, more stringent rules, this should not be interpreted as allowing the classification of some data as falling under certain categories in order to deprive them of basic data protection standards. In this sense, Article 8 of the EU Charter also applies to any processing of personal data, and not just personal data that could be ranked as having a high “level of interference” with fundamental rights.

The ECtHR has explicitly set aside arguments according to which the acquisition of “related communications data” (encompassing different instances of “traffic data”) would necessarily be less intrusive than the acquisition of the communications’ content.¹³⁷ The Court has in particular underlined that actually in some cases the processing of “related communications data” magnifies the degree of intrusion, “since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with”.

In the *Benedik* judgment, the ECtHR stressed that what could appear to be “peripheral information sought by the police, namely the name and address of a subscriber”, must in some situations “be treated as inextricably connected to the relevant pre-existing content revealing data”, as failing to do so would deny “the necessary protection to information which might reveal a good deal about the online activity of an individual, including sensitive details of his or her interests, beliefs and intimate lifestyle”.¹³⁸

The published proposal distinguishes two broad types of data: stored content data and ‘non-content data’, the latter comprising subscriber, access and transactional data.¹³⁹ It is not disputed that all these data can constitute, or at least comprise, personal data. According to the Explanatory Memorandum accompanying the proposal, personal data covered by it are “protected and may only be processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Directive for Police and Criminal Justice Authorities

¹³⁶ Ibid., p. 14.

¹³⁷ See the judgment in *Big Brother Watch and Others*, para. 356.

¹³⁸ Judgment in *Benedik v. Slovenia*, 24 April 2018 [ECLI:CE:ECHR:2018:0424JUD006235714], para. 109. On the necessity of a court order to grant access to such data, even if apparently peripheral: para. 129.

¹³⁹ Recital 20 of the proposed Regulation.

(Law Enforcement Data Protection Directive)".¹⁴⁰ Furthermore, a provision "recalls" that the regulation cannot alter fundamental rights obligations derived from Article 6 TEU.¹⁴¹

The text presented by the European Commission, nevertheless, recurrently insists that some of the categories used imply different levels of interference with fundamental rights, without detailing exactly how different would they be, while at the same time cryptically maintaining that some levels would be coincidental, and for instance that the level of interference with fundamental rights of access data "is similar to that of subscriber data".¹⁴²

Recital 23 of the draft regulation appears to attempt to account for the supposed different degrees of "interference with fundamental rights" of the described categories of data by referring to the different 'usefulness' of subscriber and access data, on the one hand, and transactional and content data, on the other, in relation to investigations and as probative material. Recognising that some types of data are most regularly sought or relied upon at different stages of investigations, however, does not as such alter the fact that any processing of personal data might be regarded as a limitation of the right to personal data protection, and must comply with all relevant standards.

Bringing in even more haziness to the reasoning, recital 30 describes transactional and content data as having a "more sensitive character", and subscriber and access data as being "less sensitive", which would legitimise that the latter might be issued or validated by prosecutors without the involvement of a judicial authority.¹⁴³ As mentioned, EU data protection law does provide special rules for certain categories of data (generally designated as "sensitive data"),¹⁴⁴ but otherwise its basic standards generally apply to all personal data, not providing for adjustments or modulations based on some perceived gradations of their minor "sensitive character".

In combination with the different treatment granted to the categories of data put forward, the proposal also resorts to a problematic distinction between European Production Orders and European Preservation Orders, according to which, as the latter do not by themselves "result in data disclosure", they would not "give rise to similar concerns" as the former.¹⁴⁵ This distinction appears to negate the fact that any processing of personal data can be regarded as a limitation of the right to personal data protection, including data collection, storage or conservation that would not result in access by another party. All relevant data protection requirements must thus be fulfilled, independent of any disclosure.

¹⁴⁰ Ibid., p. 3.

¹⁴¹ Ibid., p. 13.

¹⁴² Recital 21 of the proposed Regulation.

¹⁴³ See also European Commission (2018c), p. 16. Following the same argumentation, recital 31 of the proposed regulation notes that this would also justify orders to produce subscriber data and access data being issued for any criminal offence.

¹⁴⁴ See, in this sense, Article 9 of the GDPR (also recital 10 of the GDPR).

¹⁴⁵ Ibid., p. 22.

On the basis of this further problematic distinction, nonetheless, the Explanatory Memorandum accompanying the proposal argues that its planned review procedure can be limited to the European Production Order, and that no specific remedies are needed for European Preservation Orders.¹⁴⁶ In practice, this also means that the available remedies must be exercised always against the European Production Order (if any) and in the issuing state.

In the same vein, the proposal addresses the restriction of the rights of data subjects whose data are sought by European Production Orders in Article 11. Such a provision foresees that when the individual is not informed by the service provider upon request of the issuing authority, “the issuing authority shall inform the person in accordance with Article 13 of the Law Enforcement Data Protection Directive once there is no longer a risk of jeopardising the investigation and include information about available legal remedies”.¹⁴⁷ Yet there is no equivalent provision for European Preservation Orders, because presumably “the lesser interference with rights involved” would make that unnecessary.¹⁴⁸ It is difficult to argue this could be compliant with Article 23 of the GDPR, which establishes the conditions for any legislative measure to restrict data subject rights.

Additionally, there are a number of other important data protection issues, among which the following merit highlighting:

- **Insufficient safeguards against excessive data processing.** The proposal does not consider in enough detail measures to prevent excessive data processing, which could be imposed on both the issuing authority and the service provider. Recital 57 notes that “Member States should ensure that appropriate data protection policies and measures apply to the transmission of personal data from relevant authorities to service providers for the purposes of this Regulation, including measures to ensure the security of the data” , and that “[s]ervice providers should ensure the same for the transmission of personal data to relevant authorities”, but not enough consideration is given to need to prevent the collection of unnecessary data, or filter them out before transmission.
- **Insufficient protection for the personal data of third persons (‘collateral intrusion’).** The processing of data enabled by the proposal will potentially involve the processing of personal data of third persons (as is typically the case with data held by providers of electronic communications services, social networks, online marketplaces, other hosting service providers and providers of internet infrastructure). The proposal does not detail how such processing should be minimised, or the safeguards to be put in place. Recital 54 states that “[i]t is essential that all persons whose data are requested in criminal investigations or proceedings have access to an effective legal remedy, in line with Article 47 of the Charter of Fundamental Rights of the European Union”, but actually the rights of those whose data were not requested but are nevertheless processed should also be

¹⁴⁶ Ibid.

¹⁴⁷ Ibid., p. 20.

¹⁴⁸ Ibid.

respected. Furthermore, it needs to be taken into account that collateral intrusion might affect the communications of persons enjoying special protection, as well as special categories of data.

- **Problematic side-lining of the Law Enforcement Data Protection Directive:** Directive (EU) 2016/680,¹⁴⁹ commonly referred to the Law Enforcement Data Protection Directive, is the main EU legal instrument specifically conceived for the protection of personal data with regard to the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. It contains, therefore, special rules on issues which are absent from the GDPR such as distinguishing different categories of data subjects;¹⁵⁰ the distinction between personal data based on facts from personal data based on personal assessments;¹⁵¹ or specially adapted modulations of the rights of data subjects. Said Directive applies however only when data are processed for such purposes by ‘competent authorities’, defined as either:¹⁵²
 - any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or
 - any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Assuming the private companies impacted by the proposed e-evidence rules would not be covered by such definitions, the processing of personal data by them would fall under the GDPR. Although this instrument might be regarded in general terms as more protective than the Law Enforcement Data Protection Directive, it allows for restrictions of data subject rights which could eventually be activated without the necessary accompanying rules and modulations in line of the specific approach embodied by the Directive.

¹⁴⁹ Directive (EU) 2016/680 of the European Parliament and of the Council 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.

¹⁵⁰ See Article 6 of Directive (EU) 2016/680: ‘(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence; (b) persons convicted of a criminal offence; (c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and (d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b)’.

¹⁵¹ Ibid., Article 7.

¹⁵² Ibid., Art. 3(7).

These issues must be considered in addition to the fundamental requirement of conditioning the acquisition by a public authority of communications data from a communications services provider to prior review by a national court or independent administrative body. In this regard, the ECtHR has notably emphasised that the legal framework determining such a review must give sufficient indications to enable individuals to know the circumstances and conditions under which public authorities are permitted to request access to data.¹⁵³

As noted, in the *Digital Rights Ireland* judgment the CJEU stressed that compliance with EU fundamental rights and the principle of proportionality requires making access by competent *national* authorities to communications data dependent on a prior review carried out by a court or by an independent administrative body, to intervene following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions.¹⁵⁴ From this statement, it is not possible to infer that such compliance with EU fundamental rights and the principle of proportionality would actually be obtained by a legal instrument making possible access to data to authorities of (potentially) *any* country, even if dependent on a prior review carried out by a court or administrative body of such a Member State or third country, within the framework of procedures of their own legal frameworks. Such a possibility would directly affect, indeed, the requirement of foreseeability to be respected by all interferences with the rights enshrined in Article 8 of the ECHR.

5. Concluding remarks

Considerable pressure is mounting within the Union and at the international level to smooth law enforcement access to data across borders, as confirmed by new EU and US legislative initiatives directed at enabling the direct acceptance by private companies of data requests emanating from beyond the borders of the country where the service providers are based.

The analysis conducted in this Report has shown that any law enforcement tools for the collection of data across borders can only smooth useful data flows, and contribute to the effective investigation and prosecution of crime, to the extent that they pass the EU legality test. The CJEU's rejection of different controversial data-driven security measures confirms the importance of conducting a thorough assessment of EU (internal and external) actions' compliance with EU fundamental rights and rule of law standards, and of conducting such an assessment on time (González Fuster 2017, pp. 87-92). The scrutiny of the US CLOUD Act and of the EU proposals on e-evidence in criminal matters raises several concerns as to their compatibility with such standards.

Both instruments fall short of ensuring the dual oversight role that, under the EIO Directive and the MLAT system is assigned, first, to the authority of the issuing country and, second, to the authority of the executing country. The strength of this model of judicial cooperation results

¹⁵³ See the Judgment of the Court (Fifth Section) of 8 February 2018, *Case of Ben Faiza v France* [ECLI:CE:ECHR:2018:0208JUD003144612], para. 75.

¹⁵⁴ *Digital Rights Ireland*, para. 62.

from the interactions between authorities of the issuing and executing country, and their complementary roles played in overseeing the legality, necessity and proportionality of a cross-border request for data.

Under EU law, the competent judicial authorities of the country where the order should be executed have the duty not to execute the cross-border investigative measure when a refusal is justified by considerations related to *inter alia* fundamental rights concerns and/or the incompatibility of the order with the criminal justice standards provided by EU *and* domestic law. These standards apply to requests emanating from Member States' prosecuting authorities, which, acting under the scope of EU law, seek to access data across borders (both within and outside the EU). They must also be respected by foreign authorities requesting electronic information (pertaining to EU citizens or not), or held by private companies under EU law. Furthermore, they are binding upon the service providers holding the data sought.

The direct involvement and responsibilities of service providers in the assessments of law enforcement requests for data is problematic and deserves utmost attention. Private companies holding the data sought might, as a matter of fact, be the best placed to conduct certain technical assessments related, for instance, to whether an IP address for which content data are requested is static (i.e. pertains to a single user) or dynamic (i.e. constantly and rapidly reassigned to new users). However, this cannot pre-empt nor replace the involvement of independent judicial actors, nor substitute for their scrutiny over a cross-border request for access to data. As the Court of Luxembourg eloquently stressed, the very existence of effective judicial review, designed to ensure compliance with EU law, is "the essence of the rule of law".

Independent judicial oversight is also required to ensure that the legitimate interest of service providers in complying with a foreign authority's order to transfer data sought in the framework of a criminal investigation does not override the interests or fundamental rights and freedoms of the data subject. Service providers are surely responsible for maintaining a relation of trust and confidence with their clients, but monitoring respect of the conditions underpinning the principle of mutual trust in the EU criminal justice system is a radically different task. Only independent judicial authorities possess the necessary institutional prerogatives and professional capacity to ensure an appropriate assessment of whether a legitimate ground subsists for refusing the execution of another Member State or a third country's criminal law enforcement measure.

However, both the Commission's proposal on e-evidence and the CLOUD Act fail to ensure systematic judicial scrutiny over cross-border request for data. In the absence of a systematic independent judicial validation in the issuing phase or executing phase of a cross-border request for data, it will become difficult to ensure that the requested information is restricted to what is relevant and necessary for the prosecution of a crime.

The possibility that a company does not object to a request for data when it should do so might undermine the very objective of the measures in questions, which reportedly is to effectively enforce criminal justice through evidence-gathering across borders. Increase in conflicts of law,

and the chances of exploitation and the overuse or disproportionate issuing of orders constitute key risks that could derive from the implementation of the direct cooperation model proposed under the EU e-evidence package and the CLOUD Act. In such situations, the result may well be that the data transferred by a service provider to the prosecuting authorities will not be admitted as evidence before a criminal court.

The introduction of these new instruments could mean increasing the administrative burden in national judicial systems, with judges in the issuing countries being potentially required to review large numbers of orders, or to address complex jurisdictional issues. Pragmatically, the measures might actually trigger significant operational difficulties, and thus not solve or contribute to solving problems such as a lengthy wait to access certain data.

Another risk is that the measures could authorise practices that will have an unlawful impact on the rights to respect of private life and to the protection of personal data. The Commission proposal on the establishment of European Production and Preservation Orders, in particular, inappropriately distinguishes between different types of personal information. The lawfulness of the choice to automatically grant lower levels of privacy and data protection to subscriber and access data is doubtful, as based on the unverified assumption that these categories of information are less-sensitive by default.

The actual content of the e-evidence proposals might change as the measures tabled by the Commission undergo further inter-institutional negotiations. Despite the shortcomings highlighted in this report, the possibility also exists that further critical elements are introduced. With regard to the proposed Regulation, it is concerning to note from ongoing discussions within the Council that the EU co-legislator is considering the option of dispensing law enforcement actors from the requirement to obtain a judicial validation of data requests in a wider range of situations, including the mere existence of cybersecurity threats or a claim that obtaining validation in time would not be possible.¹⁵⁵ Similarly, and with significant data protection implications, it must be highlighted the risk that would derive from changes in the Commission proposal which would be directed at allowing for the further processing of data, for example in criminal proceedings unrelated to the original data request, or even for other uses, and including in Member States that were not at all involved in the original procedure.¹⁵⁶

¹⁵⁵ Council 2018a, p. 10 and 22.

¹⁵⁶ Ibid. p .30.

Glossary

Public authorities	
Judges	Judicial authorities who are independent from the executive branch and who exercise judicial oversight functions in the pre-trial phase, as well as independent judicial actors responsible for admitting and/or evaluating evidence in the trial phase.
Prosecutors	Judicial or administrative authorities with the competence to order the gathering of information as part of a criminal investigation, and who are responsible for coordinating criminal investigations and/or representing the prosecution in a criminal trial.
Law enforcement authorities (LEAs)	Governmental police authorities involved in criminal investigations; depending on the specific national framework of reference, this category might also include specialised law enforcement agencies (customs, anti-fraud, etc.). LEAs do not include intelligence or security services.
Central authorities	Representatives of the executive branch dealing with the issuing of cross-border requests and/or responsible for the processing (e.g. transmission or translation) of incoming foreign requests for access to data for criminal proceedings. This category includes liaison magistrates/prosecutors who are seconded abroad (e.g. to the foreign ministry by the justice ministry) and responsible for facilitating and advising on matters concerning mutual legal assistance in relation to the investigation and prosecution of transnational and cross-border crime.

Service providers	
	<p>Providers of services in the EU market and/or with a significant presence in the EU, whether or not they have their site in the EU. The providers of the following services are covered:</p> <ul style="list-style-type: none"> • Telecommunication services (voice telephony, SMS and internet access services); • Internet-based services enabling interpersonal communications such as voice-over-IP, instant messaging and web-based email services;¹⁵⁷ these also include over-the-top (OTT) communication service providers;¹⁵⁸ • Information society services that store data for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;¹⁵⁹ these include social networks (e.g. Facebook and Twitter), cloud services (e.g. Microsoft, Dropbox and Amazon Web Services), online market places (e.g. eBay and Amazon) or hosting services providers (e.g. Bluehost); and

¹⁵⁷ See the proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communication Code (Recast) (European Commission, 2016).

¹⁵⁸ They are not currently covered by the EU electronic communications framework established under Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). This might change under the new EU electronic communication and e-Privacy framework.

¹⁵⁹ Ibid.

	<ul style="list-style-type: none"> • Internet infrastructure services, such as IP address service providers and domain registrars, and associated privacy and proxy services (e.g. GoDaddy). <p>Small and medium enterprises also fall under the scope of the proposal.</p>
Legal representative	<p>A natural or legal person to be designated by a service provider established in the EU or providing services in the EU market. Service providers would be free to appoint one or more legal representatives in the EU. The representative is intended to act as an intermediary ('procedural tool') to facilitate direct cooperation and enforcement. The representative would be able and authorised by the service providers to receive, process and comply with production and/or preservation orders. It is through the representative that legal obligations under the proposal could be enforced by means of administrative sanctions. The legal representative does not need to have control or access to requested data. Service providers might decide to cumulate separate functions in one and the same person. For instance, the legal representative appointed to receive Production and Preservation Order Certificates could be the same person to act as a legal representative under Article 27 of the GDPR and the e-Privacy representative.</p>

Electronic information		
Content data	<p>The content exchanged by means of electronic communications services, such as text, voice, images and sound.¹⁶⁰ While content data include both stored and intercept (i.e. data from real-time interception of telecommunications) electronic communications content, the Commission has stressed that intercept data are out of the scope of the proposal. However, discussions within the Council suggest that the scope of the proposed regulation could be expanded to also cover this type of data (live interception).¹⁶¹</p>	
Non-content data	Metadata	<p>Data processed in an electronic communications network for the purpose of transmitting, distributing or exchanging electronic communications content. Metadata encompasses data used to trace and identify the source and destination of a communication; data on the location of the device generated in the context of providing electronic communications services; and the date, time, duration and type of communication.¹⁶² Metadata also includes, for instance, data relative to the connection, traffic or location of the communication.¹⁶³</p>

¹⁶⁰ Article 4(3)(b) of the 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) (European Commission, 2017c).

¹⁶¹ See Council of the European Union (2018b), p. 3.

¹⁶² Ibid., Article 4(3)(c).

¹⁶³ See European Commission (2018a), p. 43.

	Subscriber data	Information that allows the identification of a subscriber to a service. Examples are the subscriber's name, address and telephone number. ¹⁶⁴
	Access logs	Information that records the time and date an individual accessed a service, and the IP address from which the service was accessed. ¹⁶⁵
	Transaction logs	Information that identifies products or services an individual has obtained from a provider or a third party (e.g. a purchase of cloud storage space). ¹⁶⁶

¹⁶⁴ Ibid.

¹⁶⁵ Ibid.

¹⁶⁶ Ibid.

References

Articles, studies and reports

- Bachmaier Winter, L. (2010), "European investigation order for obtaining evidence in the criminal proceedings: Study of the proposal for a European directive", ZIS 9/2010, Zeitschrift für Internationale Strafrechtsdogmatik.
- Bárd, P. (2018), "Saving EU Criminal Justice: Proposal for EU-wide supervision of the rule of law and fundamental rights", CEPS Paper in Liberty and Security in Europe No. 2018-01, CEPS, Brussels, April (<https://www.ceps.eu/publications/saving-eu-criminal-justice-proposal-eu-wide-supervision-rule-law-and-fundamental-rights>).
- Bass, D. (2015), "As Microsoft Takes on the Feds, Apple and Amazon Watch Nervously", *Bloomberg*, 2 September (<https://www.bloomberg.com/news/articles/2015-09-02/as-microsoft-takes-on-the-feds-apple-and-amazon-watch-nervously>).
- Böse, M. (2018), "An assessment of the Commission's proposals on electronic evidence", Study for the LIBE Committee, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union, PE 604.989, September ([http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU\(2018\)604989_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf)).
- Cape, E., R.-S. Namoradze and T. Sponken (2010), *Effective Criminal Defence in Europe*, Maastricht: Intersentia.
- Carrera, S. and M. Stefan (2018), *Complaint Mechanisms in Border Management and Expulsion Operations in Europe, Effective Remedies or Victims of Human Rights Violations?*, CEPS Paperbacks, CEPS, Brussels (<https://www.ceps.eu/publications/complaint-mechanisms-border-management-and-expulsion-operations-europe-effective>).
- Carrera, S. and V. Mitsilegas (2017), "Constitutionalising the Security Union", in S. Carrera and V. Mitsilegas (eds), *Constitutionalising the Security Union: Effectiveness, rule of law and rights in countering terrorism and crime*, CEPS Paperbacks, CEPS, Brussel (<https://www.ceps.eu/publications/constitutionalising-security-union-effectiveness-rule-law-and-rights-countering>).
- Carrera, S. and V. Mitsilegas (2018), "Upholding the Rule of Law by Scrutinising Judicial Independence: The Irish Court's request for a preliminary ruling on the European Arrest Warrant", CEPS Commentaries, CEPS, Brussels (<https://www.ceps.eu/publications/upholding-rule-law-scrutinising-judicial-independence-irish-courts-request-preliminary>).
- Carrera, S., E. Guild, L. Vosyliūtė, A. Scherrer and V. Mitsilegas (eds) (2016), "The Cost of Non-Europe in the Area of Organised Crime", CEPS Paper in Liberty and Security in Europe No. 90, CEPS, Brussels, April, p. 48 (<https://www.ceps.eu/system/files/LSE%20No%2090%20Cost%20of%20Non-Europe%20in%20Organised%20Crime.pdf>).
- Carrera, S., G. González Fuster, E. Guild and V. Mitsilegas (2015), *Access to Electronic Data by Third-Country Law Enforcement Authorities*, CEPS, Brussels (https://www.ceps.eu/system/files/Access%20to%20Electronic%20Data%20%2B%20covers_0.pdf).
- Carrera, S., V. Mitsilegas, M. Stefan and F. Giuffrida (2018), *Criminal Justice and Police Cooperation between the EU and the UK after Brexit: Towards a principled and trust-based partnership*, Report of a CEPS and QMUL Task Force, CEPS, Brussels p. 43 (https://www.ceps.eu/system/files/TFR_EU-UK_Cooperation_Brexit_0.pdf).
- Daskal, J. (2016), "A new UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right", *Just Security* (blog), 8 February.

- De Capitani, E. and S. Peers (2014), “The European Investigation Order: A new approach to mutual recognition in criminal matters”, *EU Law Analysis* (blog), 23 March (<http://eulawanalysis.blogspot.com/2014/05/the-european-investigation-order-new.html>).
- Galli, F. (2018), “Fundamental rights challenges related to cross-border law enforcement access to electronic data in the framework of criminal investigations”, JUD-IT State of the Art Report No. 2, forthcoming.
- Glaser, S., A. Motz and F. Zimmermann (2010), “Mutual Recognition and its Implications for the Gathering of Evidence in Criminal Proceedings: A Critical Analysis of the Initiative for a European Investigation Order”, THEMIS 2010, Barcelona.
- González Fuster, G. (2017), ‘A Security Union In Full Respect Of Fundamental Rights: But How Effectively Respectful?’, in Sergio Carrera and Valsamis Mitsilegas (eds.), *Constitutionalising the Security Union: Effectiveness, Rule of Law and Rights on Countering Terrorism and Crime*, Centre for European Policy Studies (CEPS).
- Heard, C. and D. Mansell (2014), *The European Investigation Order: Changing the face of evidence-gathering in EU crossborder cases*, Fair Trials International (https://www.fairtrials.org/documents/NJECL_article_on_EIO.pdf).
- Hong, M. (2016), “Human Dignity and Constitutional Identity: The Solange-III Decision of the German Constitutional Court”, *VerfBlog*, 18 February (<https://verfassungsblog.de/human-dignity-and-constitutional-identity-the-solange-iii-decision-of-the-german-constitutional-court/>).
- Internet & Jurisdiction Policy Network (2017), “Cross-Border Access to User Data”, November (<https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Policy-Options-Document.pdf>).
- Jourova, V. (2018), Twitter post (<https://twitter.com/VeraJourova/status/978256311480709120>).
- Kendall, V.M. and T.M. Funk (2014), “The Role of Mutual Legal Assistance Treaties in Obtaining Foreign Evidence”, *Litigation*, Vol. 40, No. 2, Winter.
- Kyriakides, E. (2014), “Federal District Court Rules that U.S. Warrants Cover Email Content Stored Abroad”, *CDT Security and Surveillance* (blog), 1 August (<https://cdt.org/blog/federal-district-court-rules-that-u-s-warrants-cover-email-content-stored-abroad/>).
- Ligeti, K. and G. Robinson (2017), “Cross-Border Access to electronic evidence: Police and legislative challenges”, in S. Carrera and V. Mitsilegas (eds), *Constitutionalising the Security Union: Effectiveness, rule of law and rights in countering terrorism and crime*, CEPS Paperbacks, CEPS, Brussels.
- Meijers Committee (2018), “Comments on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters”, CM1809, 18 July (https://www.commissie-meijers.nl/sites/all/files/cm1809_e-evidence_note.pdf).
- Mitsilegas, V. (2016), *EU Criminal Law after Lisbon: Rights, Trust and the Transformation of Justice in Europe*, Oxford and Portland, OR: Hart Publishing.
- Mitsilegas, V. and N. Vavoula (2018), “The centrality and characteristics of privacy in the context of transnational criminal investigations”, JUD-IT Project Concept Note No. 1/October.
- Swire, P., J. Hemmings and S. Vergnolle (2017), “A Mutual Legal Assistance Case Study: The United States and France”, *Wisconsin International Law Journal*, Vol. 34, No. 2.
- Van Ballegooij, W. (2015), *The Nature of Mutual Recognition in European Law: Reexamining the Notion from an Individual Rights Perspective with a View to its Further Development in the Criminal Justice Area*, Maastricht: Intersentia, p. 354.

Van Ballegooij, W. and P. Bárd (2018), “The CJEU in the Celmer Case: One Step Forward, Two Steps Back for Upholding the Rule of Law within the EU”, *Verfassungsblog on Matters Constitutional* (<https://verfassungsblog.de/the-cjeu-in-the-celmer-case-one-step-forward-two-steps-back-for-upholding-the-rule-of-law-within-the-eu/>).

Official documents

Council of Europe (2000), “Recommendation CM/Rec(2000)19 of the Committee of Ministers to Member States on the Role of Public Prosecution in the Criminal Justice System”, Strasbourg, 6 October.

Council of Europe (2010), “Recommendation CM/Rec(2010)12 of the Committee to Member States on judges: Independence, efficiency and responsibilities”, Strasbourg, 17 November.

Council of the European Union (2010), “Proposal for a Directive of the European Parliament and the Council regarding the European Investigation Order in criminal matters: Explanatory Memorandum”, 9288/10, Add 1, 3 June.

Council of the European Union (2016a), “Review of the 2010 EU-US MLA Agreement – Examination of draft texts”, 7403/16, 7 April.

Council of the European Union (2016b), “Conclusions on improving criminal justice in cyberspace”, ST 9579/16.

Council of the European Union (2017), “Outcome of the 3546th Council meeting, Justice and Home Affairs”, Luxembourg, 8 and 9 June (<http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf>).

Council of the European Union (2018a), “Proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters - examination of a revised text”, 12113/18 Limite, 19 September 2018.

Council of the European Union (2018b), “E-Evidence: a) Regulation on European Production and Preservation Orders for e-evidence, b) Directive on legal representatives for gathering evidence + Policy debate”, 9117/18, Limite, 25 May.

Eurojust and Europol (2017), “Common challenges in combating cybercrime”, Joint Paper, Council Doc. 7021/17, 13 March.

European Commission (2014), “A new framework to strengthen the Rule of Law”, COM(2014) 158 final, 11 March.

European Commission (2015), “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, 28 April.

European Commission (2016), “Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communication Code (Recast)”, COM(2016) 590, 14 September.

European Commission (2017a), “Brief of the European Commission on behalf of the European Union as Amicus Curiae in support of neither party”, No. 17-2.

European Commission (2017b), “Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward”, Non-paper from the Commission Services.

European Commission (2017c), “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.

European Commission (2018a), “Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and

Preservation Orders for electronic evidence in criminal matters and 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”, SWD/2018/118 final – 2018/0108 (COD), 17 April.

European Commission (2018b), “Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters”, COM(2018) 225 final, 17 April.

European Commission (2018c), “Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings”, COM(2018) 226 final, 17 April.

European Commission (2018d), “Rule of Law: Commission launches infringement procedure to protect the independence of the Polish Supreme Court”, Press release, Brussels, 2 July.

European Commission (2018e), “Security Union: Facilitating access to Electronic Evidence”, Fact Sheet, April.

European Commission (2018f), “Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions: The 2018 EU Justice Scoreboard”, COM(2018) 364 final.

European Commission for Democracy through Law (Venice Commission) (2011), “Report on European Standards as regards the Independence of the Judicial System: Part II – The Prosecution Service”, 2011 Study no. 494/2008, Strasbourg, 3 January.

European Commission for Democracy through Law (Venice Commission) (2016), “Rule of Law Checklist”, Adopted by the Venice Commission at its 106th Plenary Session, Venice, 11-12 March.

European Data Protection Board (2018), “Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b)”, Brussels, 26 September.

European Judicial Network (2018), “Status of implementation of Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters”.

European Parliament Research Service (2018), “European production and preservation orders and the appointment of legal representatives for gathering electronic evidence”, Briefing.

United Nations Human Rights Council (2011), “Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework”, UN Doc. A/HRC/17/31, 21 March.

United Nations Office of the High Commissioner for Human Rights (2018), “Poland: Reforms a serious blow to judicial independence, says UN rights expert”, Geneva, 25 June.