CEPS Paper in LIBERTY and SECURITY in Europe

# 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 (updated in May 2019)


## Abstract

Crime fighting in Europe and across the Atlantic increasingly relies on the possibility for law enforcement actors to gather electronic information held by providers of cloud and telecommunication services. 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 pre-identified 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, within the EU and in the US pressure is mounting to allow law enforcement authorities' access to data outside existing judicial cooperation channels. Initiatives such as the European Commission's latest 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 report 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 proposal and the CLOUD Act's compatibility with the legality, necessity and proportionality requirements provided under EU primary and secondary law.


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

A previous version of this Report was published in November 2018. This second revised and expanded version has been prepared taking into account constructive comments provided by EU officials following the "e-evidence" package within the European Commission, Directorate General for Consumers and Justice.

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.

978-94-6138-705-9

## Contents



## List of Figures and Tables

## 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


### *Primary law standards applying to judicial cooperation for 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. Investigating and/or 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 and judicial 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 European Union. The latter has progressively developed an EU criminal justice area that also addresses issues related to 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). These supranational standards must be adhered to by Member States and third countries authorities, as well as by private companies addressed by prosecuting and/or investigating actors 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.

Different legal traditions and specific national rules also need to be taken into account to avoid that EU and international initiatives enabling prosecuting and investigating authorities to request and access data across-border conflict with national constitutional orders. The supreme courts of different EU countries have been vocal in stressing that extraterritorial effect of laws of criminal procedure, also when provided by EU law, cannot go as far as to undermine Member States' national constitutional identity. Respect of national constitutional traditions and identities is specifically mentioned in Article 4(2) of the Treaty of the European Union (TEU), and Article 67(1) of the Treaty on the Functioning of the European Union (TFEU).

### *Direct contact between Member States judicial authorities and the role of independent judicial oversight*

When it comes to intra-EU cooperation, observance of fundamental rights standards must go hand-in-hand with the need to ensure the correct functioning of the principle of mutual recognition of judicial decisions which underpins EU instruments of judicial cooperation in criminal matters.

Member States are required to trust that each other's criminal justice decisions - including cross-border measures directed at obtaining electronic information for the purpose of preventing, detecting, or combating crime - adhere to the values enshrined in Article 2 of the TEU, the EU Charter, and the safeguards found in secondary pieces of EU legislation. The principle of mutual recognition

requires the authorities of the executing country to recognise decisions from other Member States with a minimum of procedure and formality, and the grounds for non-recognition must be kept to the minimum required.

By demanding each EU country to consider all the others to be compliant with fundamental rights, mutual trust in principle prevents Member States from taking unilateral action that runs counter mutual recognition or that may compromise the primacy, unity, and effectiveness of EU law. At the same time, the free movement of judgments should not be implemented to the detriment of respect for the rule of law and fundamental rights.

Mutual recognition shall not have the effect of modifying the EU Member States' obligation to ensure respect of the fundamental rights and core legal protections provided under EU law. The Court of Justice of the European Union (CJEU) has repeatedly stressed that whereas the execution of a Member State order is deemed to constitute a manifest breach of a rule of law regarded as essential in the legal order of the other State in which enforcement is sought, or of a right recognised as being fundamental within that legal order, the refusal to recognise or enforce an order given in another Member State is justified.

The duty to verify compliance fundamental rights and the rule of law standards rely, in the first place, upon the authorities responsible for issuing or validating a decision to enforce criminal jurisdiction across borders. Most notably, EU law entrust upon the authorities of the issuing Member State the responsibility of assessing the legality, necessity and proportionality of a cross-border measure entailing access to data sought for criminal justice-related purposes.

Existing EU law instruments for mutual recognition of judicial decisions in criminal matters also foresee the involvement of competent authorities in the EU country where a criminal justice measure is to be executed. In particular, recent CJEU case law shows that the role independent judicial oversight in the executing state is central to verify the existence of those exceptional circumstances in the presence of which the principle of mutual recognition ceases to operate.

Judicial scrutiny by the executing Member State authorities remains especially crucial in a context where the Member States' criminal justice systems perform differently under important judicial independence indicators. The 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.

The authorities competent for, respectively, issuing, validating and executing a cross-border request for electronic data vary in each Member State, depending on various factors including for instance the crime involved, the stage of proceedings, and the legal instrument used as legal basis.

Depending on such factors, the authorities involved in respectively the issuing and execution of a cross-border requests for data sought in criminal proceedings might be judges or prosecutors. At the same time, it is important to recall that whether a prosecutor designated as a competent judicial authority can effectively be qualified as a judicial authority for the purposes of the application of the principle of mutual recognition in criminal matters still constitutes an open question. Previous

research and practice have shown that challenges brought against mutual recognition instruments often derive from the problem of allocation of trust in criminal justice systems.

Determining who qualifies as a competent judicial authority capable of ensuring impartial judicial scrutiny over the issuing and execution of criminal justice measures is a fundamental rule of law issues related to the principle of the separation of powers. Addressing such issue appears a crucial requirement, in particular to ensure that the EU criminal justice system is immune from politically driven (national government) interests.

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. This definition does not encompass administrative authorities such as ministries or police authorities, which are "within the province of the executive". 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.

In any case, direct contact and cooperation among the different authorities (i.e. judges and prosecutors) responsible respectively for validating or executing a cross-border request for data issued in the context of criminal proceedings represent essential preconditions to maintain the high level of trust required within the Area of Freedom, Security and Justice. Judicial cooperation and independent oversight exercised in *both* the issuing *and* executing countries can ensure that, in the extraterritorial exercise of their criminal jurisdiction, domestic and foreign investigating and prosecuting authorities remain bound by EU primary and secondary law, and respect the applicable provisions provided under national constitutional and criminal law.

### *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 is 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 substantial and procedural standards and rules 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 and mutual judicial scrutiny. Such scrutiny is in fact 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. The competent judicial authorities in the executing state which - depending on the Member State in question, on type of measure requested, and on the stage of the proceedings - might be a judge or a prosecutor, have to execute the order of another EU country within the timeframe foreseen in the Directive. At the same time, the EIO also calls upon the competent authorities in the executing state to verify whether specific grounds of legitimate refusal to recognise and execute an EIO exist.

It is precisely the considerable legal diversity as regard national legislation on evidence, coupled with the potentially far-reaching consequences of mutual recognition for constitutional protections in the field of evidence (and more specifically data) gathering and criminal justice that led to the introduction, in the European Investigation Order Directive, of a number of provisions aimed at preventing the automatic recognition of judicial decisions. Of particular relevance in this respect is the inclusion of a ground for refusal based on fundamental rights considerations, and the possibility of legal adaptation in the execution of European Investigation Order.

The existence of circumstances that might limit the automatic execution on EIO is assessed by the competent judge or prosecutor in the executing state *before* access to data is granted, These circumstances are not limited to fundamental rights issues and conflicts of laws, 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 actors gather data *outside* existing judicial cooperation channels established under the MLATs and EIO. Initiatives such the US Clarifying Lawful Use of Overseas Data (CLOUD) Act, and the Commission's proposals on e-evidence would allow investigating and prosecuting authorities to serve upon service providers orders directed at obtaining the disclosure and/or preservation of data located across borders. The achievement of this goal will depend on the establishment of a "new" public–private framework of direct cooperation. 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 authorities 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 investigating and prosecuting 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.

The procedural safeguards and rules for judicial cooperation provided under the MLA system allow to exercise a *reciprocal* judicial scrutiny over incoming LEA requests for data. 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) of the Treaty on the Functioning of the European Union. This choice is questionable and constitutes a point of controversy and disagreement among several actors and institutions commenting or reacting to the proposed regulation. Article 82 (1) does not seem to appropriately reflect the *aim* and *content* of the proposed measure. In fact, rather than promoting cooperation between judges and/or prosecutors 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 investigating or prosecuting actors' orders to produce or preserve data.

The Commission claims that the 'orders' would bring into being a 'new model' of mutual recognition. However, EU primary law appears to circumscribe the application of mutual recognition instruments to cooperation between *competent Member State authorities*. Under existing mutual recognition procedures (and in particular the EIO), the execution of other Member States' orders always depends on *the prior involvement of a competent judicial authority* (i.e. a judge or prosecutor) 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. Since there is no general assumption of reciprocal trust between public authorities and private companies, it seems difficult to qualify direct cooperation between investigating or prosecuting authorities and service providers as judicial cooperation in criminal matters. The issue appears to be very much one of lack of appropriate checks and balances.

The proposed Regulation fails in many respects to ensure systematic independent judicial oversight. According to the Commission, the authorities that would be competent to issue production or preservation orders are the same currently responsible for issuing EIOs. At the same time, far-reaching consequences derive from the choice of directly obliging service providers to produce electronic data without any systematic ex ante involvement of the competent judicial authorities in the country where the cross-border measure is to be executed.

The proposed regulation 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). Ex ante judicial validation for the access to these type of data might be however required under the law of the country where the proposed orders are to be executed. That notwithstanding, the competent judicial authorities of the Member State where the data or the company holding it is located might only be *eventually* and *accidentally* involved in the process, and solely in cases where the *service provider* decides not to execute the order. Contrarily to what is foreseen in the context of the EIO, under the proposed Regulation the competent authorities of the country where the investigative measure should be executed would not have the possibility to assess the existence of legitimate grounds of non-recongition of the order.

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 fundamental rights obligations and rule of law standards applying in the issuing Member State. Recent case law of the Court of Justice clearly shows that while non-recognition grounds may only be invoked under specific and exceptional circumstances, compliance of all EU Member States with basic fundamental rights and rule of law safeguards cannot always be taken for granted.

Under the proposed Regulation, the authorities of the member state of execution would in particular be prevented from verifying ex ante that orders issued by another EU country do not translate into infringements of fundamental rights recognised and protected at the EU level. 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.

The responsibility to assess whether an order issued in the context of a criminal proceeding is lawful (i.e. not abusive from a fundamental rights perspective) 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 assessment 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 in the issuing country) when subscriber and access data are sought. There is a risk of legalising overuse of intrusive investigative measures and even 'fishing expeditions' whereby – regardless of the seriousness of an offence - prosecutors and investigators of all EU countries would automatically issue order compelling 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 new '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

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

Marco Stefan and Gloria González Fuster

CEPS Paper in Liberty and Security in Europe No. 2018-07, November 2018
(updated in May 2019)

## 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 providers[2] 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 data[3] 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

[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.

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 access and exchange of information for criminal justice purposes to 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 competent 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 investigation, detection and prosecution of crime could improve drastically in a context where investigating or prosecuting authorities could attain electronic information directly from the service providers holding them, regardless of the location of the data, and even though the service provider or the individual concerned could be subject to another jurisdiction.

Nevertheless, far-reaching issues arise from the implementation of this cooperation model, which in practice allows prosecuting and investigating actors to directly order service providers

[5] European Commission (2018a), p. 20.

[6] European Commission (2015).

to disclose data stored abroad, without going through the competent authorities of the country where the execution of the law enforcement measure is supposed to take place.

The risk is that the execution of such a request or order violates the (national or supranational) law applying in the different countries concerned. The jurisdictional, legal and practical challenges that come from directly (i.e. non-judicially mediated) sending requests 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) Act[9] 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 regulation[10] that introduces two new data-gathering tools, namely the European Production Order and the Preservation Order. The second consists of a proposal for a directive[11] 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 investigating and 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.

[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'.

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 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 lays 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 the European Parliament, as well as Member States and US government representatives, civil society actors, service providers, legal practitioners and academics based in Brussels and Washington. A previous version of this Report was published in November 2018. This second revised version has been produced taking into account valuable and constructive comments provided by competent officials following the "e-evidence" package within the European Commission, Directorate General for Consumers and Justice.

# 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 activities[12] 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 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

[12] Article 87(2) TFEU of the Treaty on the Functioning of the European Union (TFEU).

[13] Article 82(1).

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

[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.

matters. The CJEU has made clear they need to be assessed also in conjunction with Article 47 of the Charter, which concerns access to judicial remedies in case of violation.[17]

The CJEU has progressively clarified that any limitation of the rights of respect for private life and data protection must be strictly necessary.[18] The Court in Luxembourg also established that EU and Member States' initiatives responding to the goal of fighting terrorism and crime and entailing the transfer of data across borders (and in particular to third countries) need to include rules specifying the conditions that guarantee that any limitation is limited to what is strictly necessary. These rules must be precise and clear in both content and scope, and subject to independent judicial or administrative review. Individuals must be granted the possibility to seek access to remedies in case of unlawful limitations, both within the EU and in third countries.[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]

At the national level, the specific constitutional protections accorded by different EU countries to distinct categories of personal data may also limit the possibility for (domestic and/or foreign) law enforcement authorities to directly request and obtain electronic information held by service providers and sought in the context of cross-border criminal proceedings. In fact, the grounds and circumstances justifying the issuing and execution of 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 mechanisms that apply to the issuing and execution of cross-border requests for access to data. Often, Member States' national criminal justice systems require ex ante independent judicial and/or administrative scrutiny and validation in order to prevent unauthorised intrusions of fundamental rights or strategic/sovereign interests protected at the constitutional level.[21]

---

[17] See Case C-362/14, *Maximilian Schrems,* Judgment of 6 October 2015.

[18] See Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, Judgment of 8 April 2014, and Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* and *Tom Watson*, Judgment of 21 December 2016, paras 96 and 155.

[19] See Opinion 1/15 of the Court (Grand Chamber) on the EU–Canada PNR Agreement, 26 July 2017.

[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).

[21] A Commission survey conducted prior to the publication of the e-evidence proposals indicates that "the majority of national legislations do not cover/allow that service providers established in the Member State respond to direct requests from law enforcement authorities from another EU Member State or third country. Moreover, the domestic law of only 2 Member States allows service providers established in those countries to cooperate directly with law enforcement authorities from other Member States or third countries (ES and FR)." See, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf.

The extent to which national constitutional specificities and different legal traditions provide limits to criminal justice cooperation between Member State has long constituted a matter of debate among judicial authorities, as well as between scholars. In several occasion, the CJEU has stressed that national law cannot grant a higher level of fundamental rights protection if this would compromise the primacy, unity, and effectiveness of the EU law.[22]

On the other hand, the constitutional courts of different EU countries have been vocal in stressing that extraterritorial effect of laws of criminal procedure, also when provided by EU law, cannot go as far as to undermine Member States' national constitutional identity.[23] According to some academics, it is the same principle of legality enshrined in Article 49 of the Charter, as interpreted by the CJEU, that prevents Member States from disapplying national provisions conflicting with EU law when such disapplication conflicts with the fundamental principle of legality (Mitsilegas 2014, 416-419).[24]

What relevant jurisprudential and normative developments clearly show is that the execution of an EU country's law enforcement or criminal justice measure cannot translate into an unlawful interference with a core nucleus of legal values with which all Member States must comply.[25] These appear to include the primary fundamental rights and rule of law standards which are provided by both, the EU and/or the executing member state's constitutional and legal systems (Lenaerts, 2015).

In fact, respect of national constitutional traditions and identities is specifically mentioned in Article 4(2) of the Treaty of the European Union, and Article 67(1) of the Treaty on the Functioning of the European Union. Many observers noted that the strong connections of EU criminal justice policies with the core of Member States' national sovereignty entails that protection of fundamental rights cannot be strictly limited to those harmonized by EU law (Sáenz Pérez 2018). Recent case law of the CJEU appears to support this understanding.[26]

In any event, it is clear that in order to ensure compliance with relevant primary law standards (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

[22] See Case C-399/11, *Melloni*, Judgement of 26 February 2013.
[23] See, for instance, Cort Costituzionale Italiana [Italian Constitutional Court] (ItCC), (2017), decision n. 24/2017, 6 last para.; and Bundesvarfassungsgericht (BverfG) [German Constitutional Court], 2BvE 2/08, Leitsatz 4, and; BverfG, 2 BvR 2735/114, para. 41.
[24] The question, however, remains highly debated in doctrine. See, for instance, Di Francesco Maesa, C. (2018), 'Effectiveness and Primacy of EU Law v. Higher National Protection of Fundamental Rights and National Identity: A look through the Lens of the Taricco II Judgement', Eucrim, Issue 1/2018, p. 50-56.
[25] The most recent EU normative developments in the area of criminal justice also appear to confirm the ongoing trend towards an increasingly restrictive interpretation of the powers of national authorities to limit the operationalisation of the mutual recognition principle. See the newly adopted Regulation (EU) 2018/1805 of the European Parliament and of the Council on the mutual recognition of freezing orders and confiscation orders. The EP and Council agreed, among other things, on the inclusion of a ground for non-recognition based on fundamental rights, but under very strict conditions.
[26] See Case C-42/17, *Taricco II*, Judgment of 5 December 2017.

borders must plan for the involvement of *effective judicial oversight mechanisms* (Carrera and Stefan, 2018, pp. 13-18).

These oversight mechanisms must be provided for in order to ensure that the rights to an effective remedy and to effective judicial protection, as enshrined respectively in the EU Treaties (Art 19 TEU) and the EU Charter (Art. 47) are delivered in practice (see section 2.2 infra). On the one hand, such mechanisms are necessary to monitor that the domestic requests for gathering of data is consistent with EU fundamental rights and rule of law standards that apply to criminal investigations, and access to electronic information in this specific context. On the other, they help preventing conflicts of law within the EU, most notably by allowing for the execution of a foreign order in line with the procedures and safeguards prescribed under the national law of the concerned country.

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 Judicial cooperation in criminal matters and the role of independent judicial scrutiny over cross-border data requests

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. By virtue of the principle of mutual recognition, the authorities of the executing country are required to recognise decisions from other Member States with a minimum of procedure and formality, and the grounds for non-recognition must be kept to the minimum required.

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). Such a presumption is generally referred to as *mutual trust* (Van Ballegooij, 2015, p. 354). By demanding each EU country to consider all the others to be compliant with fundamental rights, mutual trust in principle prevents Member States from taking unilateral action that runs counter mutual recognition (Bárd and van Ballegooij, 2018a).

While the AFSJ is built upon the presumption that all Member States comply with fundamental rights and the rule of law, it is also clear that mutual trust is not blind trust, and that mutual

recognition is not unconditional. If fact, the automatic execution of cross-border judicial decisions under the mutual recognition principle remains 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 protected 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 defer, and eventually non-recognise and/or non-execute 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.[27]

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.[28]

Most recently, the Court has also indicated 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 material[29] demonstrating 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 and impartiality of those courts.[30]

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

[28] Ibid., para. 104.

[29] 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, para. 79.

[30] Ibid., para. 58.

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). The CJEU confirmed that it is the responsibility of national courts of the state of execution 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).

In fact, national courts are to ensure "the full application of European Union law (…) and (…) judicial protection of an individual's rights under that law".[31] 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 measure is to be executed. However, systemic dysfunctionalities 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.[32]

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 Juízes Portugueses* of 28 February 2018,[33] 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.[34]

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

[31] See Opinion 1/09 of the Court (Full Court), 8 March 2011.

[32] See United Nations Office of the High Commissioner for Human Rights (2018).

[33] Case C-64/16.

[34] Ibid., paras 35 and 36 (emphasis added).

jurisdiction is compulsory, whether its procedure is *inter partes*, whether it applies rules of law and whether it is independent".[35]

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 in fact 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.

The challenge then is to identify precisely which are the authorities capable of providing effective legal protection in the context of a criminal proceeding. The current definitions and concepts of 'competent judicial authority' and 'court having jurisdiction in criminal matters' – also for the purpose of evidence gathering - are not always clear in EU law, let alone under national law of different EU countries. The authorities competent for, respectively, validating, receiving and executing a criminal justice measure - including requests for data sough in criminal proceedings - vary in each Member State, and depending on various factors including for instance the crime involved, the stage of proceedings, and the legal instrument used as legal basis.[36]

Depending on such factors, the authorities involved in respectively the issuing and execution of a cross-border requests for data sought in criminal proceedings might be judges and prosecutors. Recent scholarly analysis has shown how, at the national level, it has become increasingly difficult to demarcate the labour division between administrative and criminal authorities vested with investigative powers (Sellier and Weyenbergh 2018, p. 22). At the same time, it is important to recall that whether a prosecutor designated as an compentent judicial authority can effectively be qualified as a judicial authority for the purposes of the application of the principle of mutual recognition in criminal matters still constitutes an open question.[37]

Determining who qualifies as a competent judicial authority capable of ensuring impartial judicial scrutiny over the issuing and execution of criminal justice measures is, however, a fundamental rule of law issues related to the principle of the separation of powers.[38] Addressing such issue appears a crucial requirement, in particular to ensure that the EU criminal justice system is immune from politically driven (national government) interests. Previous research and practice have shown that challenges brought against mutual recognition

[35] Ibid., para. 38.

[36] See, European Judicial Network, Judicial Atlas, http://www.eurojust.europa.eu/Practitioners/European-Judicial-Network/Pages/Judicial-Atlas.aspx.

[37] See, reference for a preliminary ruling from the High Court (Ireland) made on 7 November 2018 – Minister for Justice and Equality v ND, (Case C-685/18).

[38] In this regard, it is worth noting that only recently the Maltese government moved towards the separation of powers in the judiciary though the adoption of new legislation intended tol ensure "separation of the prosecution and the advisory roles" of the country's attorney general, a job that has thus far involved being both the country's chief prosecutor and a political adviser to the government. See, https://www.politico.eu/newsletter/brussels-playbook/politico-brussels-playbook-presented-by-bp-summits-gotta-give-eus-in-charge-maltas-colonial-rule-of-law-baggage/.

instruments (and in particular the EAW) often derive from the problem of allocation of trust in criminal justice systems (Guild and Hernanz, 2013, p. 23).[39]

And yet, 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.[40] This definition does not encompass administrative authorities such as ministries or police authorities, which are "within the province of the executive".[41] 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).

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).

The CJEU has in fact clearly established that access to data for law enforcement purposes necessitates *independent scrutiny*. Judicial oversight is required to verify that the gathering of electronic information can bring an *effective contribution* to the prosecution of a specific crime. This happens when, in a specific case, objective evidence is given that a relationship exists between the data sought and the person likely to be involved in the commitment of a crime.[42] The competent law enforcement actors are required to submit a 'reasoned request' from which it can be inferred that access to the data is strictly necessary for the purpose of prevention, detection or prosecution of crime.[43] The reasoned request must be reviewed either by a court or by an independent authority prior to data access by the prosecuting authorities.

The European Court of Human Rights (ECtHR) has recently determined that in an EU Member State the acquisition by a public authority of communications data from a communications services provider requires that data access be subject to prior review by a court or independent administrative body.[44] 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

[39] The authors observed that "if judges and juries had mutual trust in the police then there would be no need for a trial, the defendant would obviously be guilty because the police say so and the judge and jury trust the police".
[40] In Cases C-452/16 PPU *Poltorak* of 10 November 2016, C-477/16 PPU *Kovalkovas* of 10 November 2016 and C-453/16 PPU *Özcelik*, of 10 November 2016.

[41] Ibid., para. 35.

[42] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB* v *Post-och telestyrelsen* and *Secretary of State for the Home Department* v *Tom Watson, Peter Brice, Geoffrey Lewis*.

[43] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd* v *Ireland*, 8 April 2014, para. 62.

[44] Judgment of the Court (First Section) of 13 September 2018, *Case of Big Brother Watch and Others* v *the United Kingdom,* App. No. 58170/13, 62322/14, 24960/15; see especially paras 463, 466 and 467. It should be pointed that that judgment considers the compatibility with ECtHR standards of three different, discrete regimes, and for each of them carefully identifies the relevant interference(s) with fundamental rights, the compatibility of which had to be assessed separately, in the Court's view.

Rights (ECHR) to be "in accordance with the law" cannot be regarded as fulfilled. The ECtHR reached such conclusion by taking into account the referred CJEU case law, in particular the *Digital Rights Ireland* judgment.[45]

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 rights recognised in Article 10 of the ECHR,[46] 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 investing and prosecuting actors 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 speeding up the procedures for gathering 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 establishing a direct contact between the competent judicial authorities of the different Member States concerned by the proceeding. Cooperation and direct contact among judicial authorities of the different Member States concerned by a cross-border proceeding remains one of the cornerstones of judicial cooperation in criminal matters within the Union and represents an essential precondition to maintain the high level of trust required within the Area of Freedom, Security and Justice (Janssens 2013, p. 246).

Judicial cooperation among competent authorities in both the issuing and executing state allows to adequately assess the existence of the circumstances in the presence of which the principle of mutual trust exceptionally ceases to operate. As noted above, independent judicial scrutiny by executing Member States' authorities appears especially crucial in a context where EU countries' criminal justice systems perform differently under important judicial independence indicators.[47] 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.[48] The reasoned proposal submitted by the Commission to

[45] It might be useful to recall that in such judgment the CJEU in particular discusses an obligation imposed on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications (para. 34), but also the access of the competent national authorities to the data (para. 35).

[46] Ibid., paras 496-499.

[47] 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.

[48] 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 Stares on judges and Recommendation Rec(2000)19 on

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 judiciaries[49] prove that restrictions imposed upon judicial independence in one Member State have far-reaching consequences for other countries of the Union.

Against this backdrop, it appears that the involvement of independent judicial oversight is first of all required to ensure that data located across the border are requested by law enforcement 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.

Ascription of judicial authorities as the depositary of trust in EU criminal matters ultimately depends on the division of powers principle,[50] which presumes their structural independence in assessing whether the execution of another Member State's order will not infringe EU principles, laws and values.[51] However, ensuring the high level of trust required in the AFSJ becomes challenging in the absence of the possibility for competent judicial authorities in the requested state to receive and validate the requests for 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

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.

[49] 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).

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

[51] 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.

respect the sovereignty of the foreign country on whose territory an investigative measure needs to be implemented.[52]

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 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.[53] As submitted by the Commission, the Agreement "largely relies on existing and future bilateral agreements with particular [Member States]".[54] If the Agreement supplements existing bilateral agreements, "the latter do not operate in isolation from Union Law".[55] 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.[56]

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

[52] European Commission (2018a), p. 22.

[53] See Article 3(2)(a) of the EU–US MLA Agreement.

[54] European Commission (2018a), p. 23.

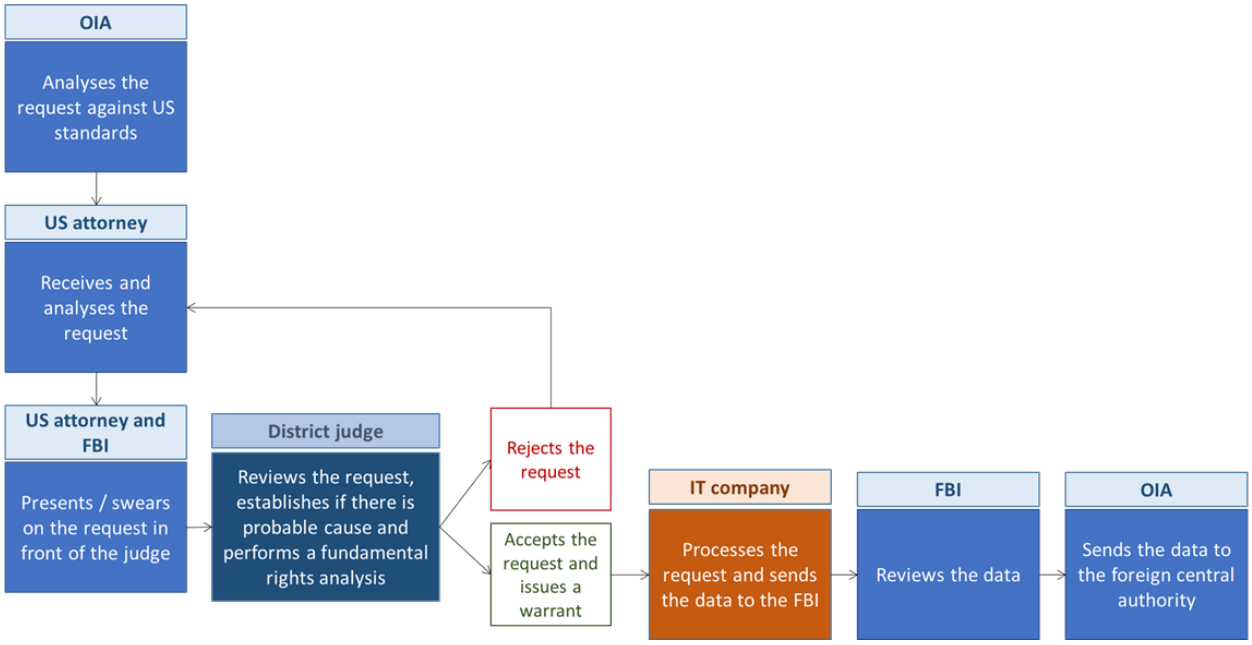
[55] Council of the European Union (2016a), p. 3.

[56] Ibid.

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.

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 Amendment[57] and specific provisions of statutes, such as the Electronic Communications Privacy Act (ECPA), which protects wire, oral and electronic communications in transit.

[57] 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.

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 electronic communications might only be produced when a US federal judge has been satisfied of the existence of "probable cause".[58]

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.[59] 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.[60] 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

[58] 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.

[59] 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.

[60] 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).

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 emerges if foreign investigators' requests for electronic data falling 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.[61] 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 Act [62] 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,[63] 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) 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 an MLAT*, 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.[64]

[61] Case C-362/14 *Maximillian Schrems* v *Data Protection Commissioner*, Judgment of 6 October 2015, paras 70–72.

[62] Section 103 of the CLOUD Act.

[63] Section 105 of the CLOUD Act.

[64] 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) (emphasis added).

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.

In its *amicus curiae* brief submitted on behalf of the EU to the Supreme Court in the *Microsoft Ireland* case, [65] 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".[66] 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.[67] 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).

[65] See European Commission (2017a).

[66] Ibid., p. 9.

[67] European Commission (2018a), p. 78.

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 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.[68] 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.[69] 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

[68] 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.

[69] 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.

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.

Mutual legal assistance agreement provide procedural safeguards that allows to deal with conflicts of laws and jurisdiction in cross-border requests for access to electronic data. Excluding the possibility to exercise reciprocal judicial scrutiny that the MLAs system ensure over incoming LEA requests for data would instead jeopardise the possibility to safeguard fundamental rights standards provided under EU primary 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.[70] 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 seven Member States.[71] Except for Denmark[72] and Ireland,[73] 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.[74]

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."[75] 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

[70] Council of the European Union (2016a).

[71] These were Austria, Belgium, Bulgaria, Estonia, Luxembourg, Slovenia, Spain and Sweden.

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

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

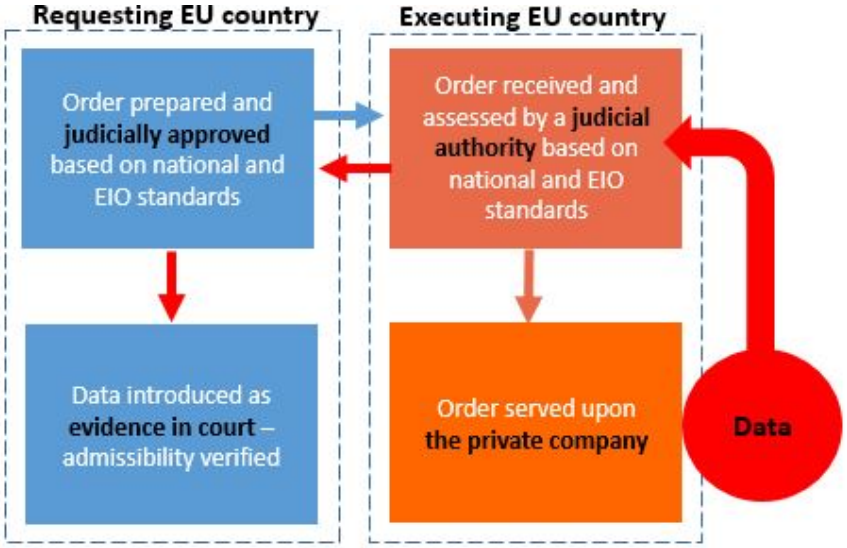
[74] European Judicial Network (2018).

[75] See Eurojust and Europol (2017).

The EIO Directive creates a "single, efficient and flexible instrument"[76] 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.[77] 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.[78] 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 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.

[76] Council of the European Union (2016b), p. 2.

[77] 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.

[78] 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.[79] The EIO should be executed within the strict time limits provided in the Directive.[80] 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.[81] 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"[82]

The EIO Directive contributes to enhancing criminal justice 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.[83] 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".[84]

[79] 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.

[80] Article 12(3)–(5) of the EIO Directive).

[81] Article 12(2-4) of the EIO Directive

[82] Article 12(1) of the EIO Directive.

[83] 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.

[84] Recital 11 of the EIO Directive.

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,[85] and when the judicial decision of the issuing Member State may give rise to proceedings before a court having jurisdiction in criminal matters. An EIO may be also be issued in proceedings brought by administrative authorities in respect of acts which are punishable under the national law of the issuing State by virtue of being infringements of the rules of law and where the decision may give rise to proceedings before a court having jurisdiction, in particular, in criminal matters.[86] 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.

The authorities competent for issuing, validating, or executing an EIO may include, depending on the different Member States concerned and the specific circumstances of the case, both judges and prosecutors. 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 scrutiny by the competent authority of the executing state with regard to the legality and fundamental rights compatibility of the investigative measures requested through the EIO. In fact, Art. 11(1) of the EIO Directive included the thresholds under the law of the executing member state or catalogue offences as a non-recognition ground. Furthermore, the EIO Directive appears to have maintained the double criminality requirement for orders concerning the production of more sensitive data (e.g. content data and, in some cases, traffic data) and related to facts falling outside the list of the 32 offences for which double criminality was abolished.[87]

Therefore, besides introducing a demand-based system for conducting cross-border investigative measures based on swift procedures and minimum formalities, the EIO Directive sets out a number of new rules which temper the automaticity in the execution of the Orders with the objective of guaranteeing a set of supranational standards while also ensuring compliance with the legal and constitutional system of the executing Member State. The considerable legal diversity as regards national legislation on evidence, coupled with the potentially far-reaching consequences of mutual recognition in the field of evidence for national constitutional traditions and the protection of fundamental rights, have in particular

[85] 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.

[86] Article 4 of the EIO Directive.

[87] European Parliament (2019), Commitee on Civil Liberties, Justice and Hoem Affairs, 2nd Working Document (B) on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) - Scope of application and relation with other instruments, pp. 2-4.

led to the inclusion in the text of the Directive of several provisions aiming to prevent automatic mutual recognition (Carrera et al., 2016, p. 50).

The executing authority might decide not to recognise and/or 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".[88] The introduction of specific provisions on comparable measure in the EIO is justified in light of the diversities of national measures to obtain evidence. In substance, the EIO Directive aims at increasing mutual trust and cooperation between pre-identified competent authorities of EU Member States, while at the same time preserving the specificities of the national systems and their legal culture.

The EIO is also has a full ground of refusal based on fundamental rights. Whereas previous instruments of mutual recognition in criminal matters only included a general reference to the Charter, this piece of EU legislation expressly requires judicial authorities to verify whether the execution of an EIO is compliant with fundamental rights standards.[89] 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.[90]

Competent authorities 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.[91] 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

[88] Article 10(3) of the EIO Directive.

[89] Article 11(1)(f) of the EIO Directive.

[90] Recital 19 of the EIO Directive.

[91] Article 11 of the EIO Directive.

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".[92]

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.[93] 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".[94] 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 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.

The rules and procedures for judicial cooperation incorporated in the EIO Directive allow *electronic data* collected as part of a cross-border criminal investigation to qualify as *evidence* accepted as 'admissible' before a court of law. Similarly to the MLATs, the channel of formal judicial cooperation provided under the EIO allows to verify that the right authorities have been involved, and that the substantial safeguards and procedural rules applying to the issuing and execution of a request for data have been taken into account in the different countries concerned by a cross-border criminal proceeding.

Bypassing the channels of direct cooperation between competent authorities provided under the EIO would instead increase the risk that admissibility of data obtained across borders is successfully challenged in court. Failure to comply with the rules and modalities for information

[92] Article 11(1)(h) of the EIO directive.

[93] Article 14 of the EIO Directive.

[94] Article 1(3) of the EIO Directive.

gathering that apply in the country where the investigative measure is addressed might well constitute a ground for exclusion of evidence (Seller and Weyembergh 2018, p. 55).

The EIO Directive is a key legal development in the field of judicial cooperation between EU Member States and in the field of the development of the application of the principle of mutual recognition in criminal matters more broadly. As highlighted by previous research, the Directive reconciles the need to operationalise the mutual recognition principle with fundamental rights and proportionality checks in the executing Member State. According to previous research undertakings, the EIO introduces new *EU legal standards* in as far as it reflects a constitutional settlement between Member States, and to the extent that it sets out clear limits and parameters to the operation of mutual recognition (Carrera et. al, 2016, p. 54).

In particular, the proportionality and fundamental rights safeguards provided under the internal legal and constitutional order of the issuing *and* executing Member State safeguards, as well as the judicialisation of mutual legal assistance constitute clear advances in the law of mutual recognition. The EIO reflects how EU primary law standards and the respect of core national constitutional specificities have been currently embedded in existing criminal justice instruments for cross-border cooperation in the field of evidence gathering.

## 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"[95] 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.

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

| Service providers concerned | |
|---|---|
| **E-evidence proposals** | **CLOUD Act** |
| All digital service providers, including<br>• electronic communications (covering telecommunication) service providers;<br>• information society service providers; and<br>• providers of internet infrastructure services and marketplaces. | US companies, including<br>• electronic communications service providers (such as email providers); and<br>• remote computing service providers (including certain cloud storage providers). |
| They fall under the scope of the e-evidence proposals as long as they **offer services in the EU market**, even if<br>• the *data are stored abroad* (e.g. in the US);<br>• the main site of the company is *not established in the EU*; and<br>• the *service is provided from abroad*. | They fall under the scope of the CLOUD Act if **their main site is in the US**, when:<br>• 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 *stored in the US*;<br>• the data are *stored abroad* (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).[96]

## 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 address both the legal and operational obstacles deriving,

[95] See European Commission (2018d), p. 4.

[96] See the glossary in this report.

on the one hand, from the voluntary nature of current service provider's cooperation with LEAs, and on the other hand from the 'mediated' model of cross-border cooperation for access to data under 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 European Agenda on Security[97] and they advanced in parallel with other (different) initiatives put forward under the so-called Security Union strategy.[98] 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.[99]

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.[100] 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.[101] 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.[102]

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

[97] 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).

[98] See European Commission (2018e).

[99] Council of the European Union (2016b).

[100] European Commission (2017b).

[101] Ibid., p. 2.

[102] European Commission (2018a), p. 46.

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".[103]

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 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.[104] 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.[105]

## 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(1)TFEU as a legal basis for the proposed regulation on European Production and Preservation Orders for electronic evidence in criminal matters. The choice of this specific legal basis has been a point of controversy and disagreement, including among several communities of legal practitioners[106] and civil society actors commenting or reacting to the proposed regulation.[107]

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. The envisaged proposal seeks to confer extraterritorial jurisdiction on the prosecuting and investigating authorities of one Member State directly to address a private entity in another Member State, but it does not involve the authorities of the Member State in which is situated the undertaking in receipt of the request.[108]

---

[103] Ibid., p. 47.

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

[105] Council of the European Union (2017).

[106] See, Deutcher Richterbund (2018), "Stellungnahme des Deutschen Richterbundes zur Europäischen Verordnung zu elektronischen Beweismitteln in Strafsachen", 4 July 2018 (https://www.drb.de/positionen/stellungnahmen/stellungnahme/news/618/).

[107] See, European Digital Rights (EDRi) (2018), "Civil society urges Member States to seriously reconsider its draft position on law enforcement access to data or "e-evidence"", 5 December 2018 (https://edri.org/files/20181203_e-evidence_civilsocietyletter.pdf).

[108] See Council of Bar and Law Societies of Europe (CCBE) position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, 19 October 2018.

According to the Commission, the authorities that would be competent to issue production or preservation orders are the same currently responsible for requesting, validating and issuing EIOs. The proposal foresees that authorisation by a court in the issuing country would be required only when a Production Order concerns the production or preservation of specific types of (i.e. transactional or content) data. The involvement of a court would instead not be required as far as non-content data, and notably subscriber and access data, are concerned. It is proposed that disclosure of the latter types of information could be ordered directly by prosecutors.[109] Thus, independent judicial scrutiny by a court would not automatically apply in the country issuing the order when these target specific types of supposedly 'less sensitive' data (i.e. subscriber and access data). The same applies to European Preservation Orders, which could also be issued without independent judicial validation, and regardless of the types of data concerned.

The proposed regulation neither foresee the systematic involvement of the competent judicial authorities of the Member State where the data, or the company holding it, are located or appointed their legal representative. This represents the main qualitative difference between the proposed orders and already existing mutual recognition instruments in criminal matters. According to the Commission's proposal, judicial actors of the EU country of execution 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).

It has to be acknowledged that Article 82(1)(a) of the TFUE foresees the possibility to adopt EU measures to lay down rules and procedures for ensuring recognition throughout the Union of all forms of judgments. At the same time, it seems questionable that the execution of a Member State authority's decision to access personal data by a private company can be qualified either as judicial cooperation, or as a form of mutual recognition of judicial decisions in criminal matters. Even if similar modalities of cooperation have been previously applied in judicial cooperation in civil matters, doubts have been expressed as to the possibility to extent the same logic to cooperation in the field of criminal law.[110]

In this regard, it is worth mentioning that Member of the European Parliament's LIBE Committee have expressed concerns about the need to interpret EU primary law provisions related to criminal justice strictly in order to avoid a "non-solicited and hidden Treaty change". They also referred to an opinion expressed by the CJEU Attorney General Mengozzi, according to which qualifying cooperation between law enforcement and private service providers as

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

[110] As observed in the e-evidence – Questions for Written Answer to COM – Follow-up to Shadows' Meeting 09/10/2018, p. 1.

judicial cooperation could amount to a "generous"- that is overly broad - interpretation of the Treaty.[111]

As expressly noted by representatives from eight Ministries of Justice of EU member states (Germany, The Netherlands, Czech Republic, Finland, Latvia, Sweden, Hungary and Greece),[112] the "tried and tested practice of mutual recognition" in criminal matters would be "largely abandoned" in a context where the judicial authorities of Member States concerned by a cross-border proceeding are no longer required to cooperate among them. The question seems very much one of checks and balances within the EU criminal justice system. It is among judicial authorities that a relationship based on reciprocal trust is established under EU criminal law – there is no general assumption of reciprocal trust between public authorities and private companies.

Indeed, there is no general requirement in the EIO Directive for a judge to authorise the issuing or the executing of the measure, and in some cases the involvement of a prosecutor is sufficient. However, under current mutual recognition instruments, decisions *come from a judicial (or equivalent) authority* in the issuing state and *are addressed to a judicial authority* (i.e. a judge or a prosecutor) in the Member State where the addressee or the object concerned by the measure is located. The EIO systematically relies upon *direct contact between competent judicial authorities* in both the issuing and executing state. Such direct contact is designed to allow for the assessment of the existence of the circumstances in the presence of which the principle of mutual recognition exceptionally ceases to operate. In the European Investigation Order Directive, these circumstances also encompass cases where the execution of an order would unlawfully impact individuals' right to privacy, fair trial, rights of the defence and the right to an effective remedy as enshrined in the EU Charter of Fundamental Rights.

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. It is true that even the authorities competent to issue and execute EIOs are not always independent judges *sensu strictu* (and might, under certain circumstances, also be prosecutor). At the same time, under the proposed regulation the authorities which are responsible to recognise and execute an EIO in the state to which the order is addressed would not be involved in the procedure when the service providers directly comply with a European Production or Preservation Order issued by another EU country (see subsection 4.2.3 below).

[111] See European Parliament, LIBE Committee, 2nd Working Document (A) on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Scope of application and relation with other instruments, p. 5.

[112] Ministries of Justice of Germany, The Netherlands, Czech Republic, Finland, Latvia, Sweden, Hungary, Greece (2018), Letter to Mrs Věra Jourová, 20 November (https://cdn.netzpolitik.org/wp-upload/2018/11/2018-11-20_Justizminister-Brief_EEvidence1.pdf).

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 judge or a prosecutor in the Member State issuing an order alone is sufficient to ensure that the person concerned by a criminal justice 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."[113] 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.

The need to ensure the involvement of judicial authorities in the *different* Member State concerned by a cross-border criminal proceeding clearly emerges from the wording of Article 82 of the TFEU. In the case of the draft EU-Canada Passenger Name Records (PNR) Agreement, the Court of Justice of the European Union expressly underlined that Art. 82 was not an appropriate legal basis, as the competent Canadian authority does not qualify a judicial authority.[114] Arguing that main objective of the proposal is precisely not to involve the judicial authority in the country where the order is addressed, the European Data Protection Board has also questioned the appropriateness of the Commission's choice of legal basis (EDPB 2018, p. 4).

In its overall favourable opinion towards the proposed Regulation, the European Judicial Network (EJN) suggested that authorities that are currently competent to request data should also be competent for issuing the production or preservation order. At the same time, the Opinion also acknowledged that concerns regarding the right legal basis in Article 82 of the TFEU could arise from allowing law enforcement authorities (in same case including prosecutors) to order service providers across borders to directly produce or preserve data (EJN, 2018, p. 2-3).[115]

Direct contacts between judicial authorities of the countries where an order is issued and needs to be executed, and the systematic oversight of a competent judicial or equivalent authority in the executing state capable of ensuring effective remedies for individuals affected by the orders constitute critical conditions that would make the proposed regulation more appropriately match the requirements of an instruments of judicial cooperation in criminal matters. These factors would also ensure that the fair trial principles outlined in the EU Charter of Fundamental Rights and the rights of suspects provided under EU secondary legislation are adequately protected.

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

[114] See Opinion 1/15 of the Court (Grand Chamber) on the EU–Canada PNR Agreement, 26 July 2017, para. 103, and; para 108 of the opinion of the advocate general in this case.

[115] European Judicial Network, Conclusions of the EJN e-Evidence Working Group on the proposals for a Production and Preservation Order and Appointment of a legal representative, pp. 2-3.

Based on the above, it is worth asking whether Art. 87 of the TFEU (enabling the adoption of legislation in the field of police cooperation among the Member States in relation to the prevention, detection and investigation of criminal offences) would better reflect both the main *aim* and *content* of the e-evidence proposals.

According to the Commission's proposals, police is not authorised to issue orders without validation by a judicial or equivalent authority (including both judges or prosecutors). At the same time, rather than facilitating the mutual recognition of judicial decisions within the Union, the proposed regulation appears to mainly be directed at enabling investigating and prosecuting authorities (including not only judges, but also 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. However, it is important to remember that not in all EU countries prosecutors qualify as independent judicial authority. While in some Member States (e.g. Belgium, Bulgaria, France, Italy, and Romania) prosecutors are magistrates and enjoy a similar status to judges, in many other European countries prosecutors are part of the judiciary *sensu lato,* or may be even considered part of the executive. In common law jurisdictions, furthermore, prosecutors are entirely separate from the judiciary, and operate much as any other represented party would operate before the courts.[116]

As explicitly stressed by the CJEU, under EU law the choice of legal basis for any EU action must be supported by objective factors, "amenable to judicial review".[117] 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".[118] 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*".[119]

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

[116] European Netwrok of Councils for the Judiciary (2016), Independence and Accountability of the Prosecution, ENCJ Report 2014-2016.

[117] Opinion 1/15 of the Court (Grand Chamber) on the EU–Canada PNR Agreement, 26 July 2017, para. 55.

[118] Case C-178/03 *Commission of the European Communities* v *European Parliament and Council of the European Union*, para. 1 (emphasis added).

[119] Ibid. (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).

In relation to the protection of personal data, the Commission's proposals do explicitly refer to the need to respect the fundamental right to the protection of personal as enshrined both in the EU Charter of Fundamental Rights and the Treaties (Article 16(1) of the TFEU). As mirrored in Recital 56 of the proposed regulation, this imperative is to a large extent addressed by recalling that it is the responsibility of Member States to ensure that personal data are protected, by making sure they are only processed in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680. This nevertheless leaves open the question of whether the protection offered by these instruments (adopted on the basis of Article 16(2) of the TFEU) shall be deemed sufficient in light of the new data processing practices brought about by the proposals.

### *4.2.2 Concerns over necessity, legality and proportionality*

The proposed regulation is said to have a limited scope.[120] 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.[121] 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.[122]

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

[120] See pp. 5-6 of the draft regulation Explanatory Memorandum

[121] Article 5(3) of the proposed regulation.

[122] Case C-207/16 *Ministerio Fiscal*, para. 95 and following.

crimes".[123] 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,[124] the CJEU recognised that legitimate derogations to the principle of confidentiality of electronic communications are not strictly limited to the fight against serious crime, but can be admitted also 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. Independent 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.[125] 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 |

[123] See European Commission (2018a), p. 44.

[124] Case C-207/16 *Ministerio Fiscal*.

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

| | | |
|---|---|---|
| **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.

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.[126] 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".

There is a risk of legalising overuse of intrusive investigative measures and even 'fishing expeditions' whereby regardless of the seriousness of an offence prosecutors and investigators of all EU countries would automatically issue order compelling service providers to produce or preserve large troves of non-content data. Yet, without judicial validation by an independent judge in the issuing state, 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. Also, under the proposed regulation the authorities of the Member State where the order is to be executed would not have the possibility to recur to a less intrusive investigative measure, even in cases where such less intrusive measure would achieve the same result of a production of preservation order. Additionally, the proposal in its current shape does not foresee an 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.

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

[126] See European Commission (2018a), p. 14.

would lead to the collection of data that can produce probatory material before a criminal court.

The Commission previously highlighted that direct requests from law enforcement authorities to service providers are not expressly foreseen under most national laws of criminal procedure, and noted that data obtained through cross-border direct public-private cooperation might not be admitted as evidence in a later criminal trial (Commission 2016). Despite these concerns, the e-evidence proposal does not contain any provision on admissibility, but only acknowledges the widely divergent admissibility rules between the Member States (Seller and Weyembergh 2018). There is a risk that the data collected under the proposed instruments 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 existence of potential immunities or privileges.[127] 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.[128] 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)).[129] 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.[130] True, the proposed regulation also allows service providers to object to the automatic execution of the

[127] Article 5 of the proposed regulation.

[128] Article 7 of the proposed regulation.

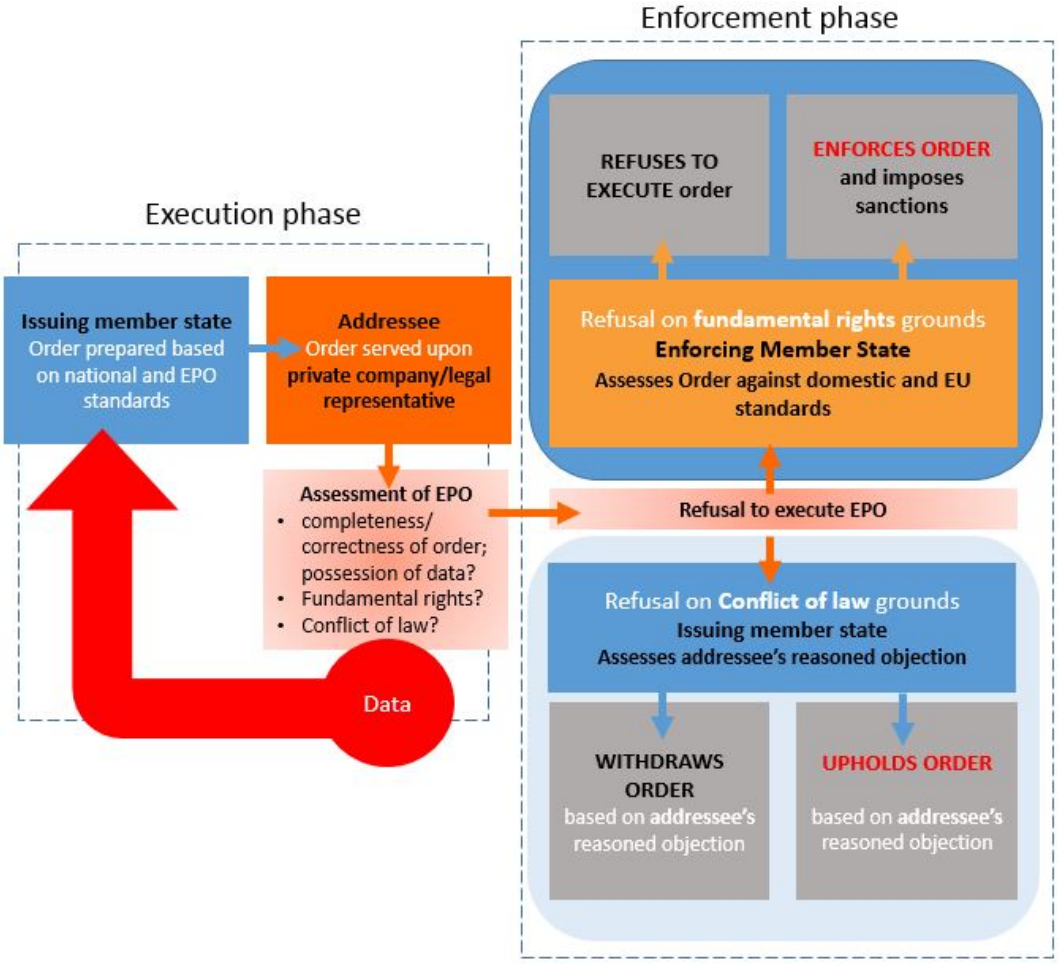
[129] Ibid., Articles 9 and 10.

[130] Ibid., Article 13.

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.[131] Outside these cases, any ISP or company refusal to execute the order is automatically considered a case of "non-compliance".

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.

*Figure 3. Execution and enforcement of the proposed orders*




*Note:* EPO = European Production/Preservation Order.
*Source*: Authors elaboration

## 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

[131] Ibid., Article 9.

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).[132] 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.[133]

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".[134] 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.[135]

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.

[132] 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.

[133] Article 5 of the proposed regulation.

[134] Recital 46 of the proposed regulation.

[135] See United Nations Human Rights Council (2011).

### 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. 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.[136] 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 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.[137]

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

[136] Judicial scrutiny is not necessary for other types of data.

[137] Article 18 of the proposed regulation.

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:

- the lack of formal judicial authorisation and a substantial threshold (when the orders concern content and transactional data);[138]
- 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;[139] and
- the outreach of the order beyond the scope of the regulation (when the order is issued outside the pre-trial or trail phase, or when it does not target service providers providing services within the Union).[140]

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. As a consequence, the service provider might be forced to execute an order even when such a measure has not been adopted in accordance with the law of the issuing Member State.

Furthermore, 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).[141] 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

[138] Ibid., Article 14(2), (4)(a–b) and (5)(a).

[139] Ibid., Article 14(4)(f) and (5)(e).

[140] Ibid., Article 14(4)(e) and (5)(d).

[141] 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.

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 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"[142] 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 that the one typically required to request and obtain data across borders directly through existing MLA channels.

[142] 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.[143]

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.[144]

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

[143] Article 17(1) and (3) of the proposed regulation.

[144] 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"[145] and a series of "national tools" developed since by some Member States and third countries.[146]

The proposal, however, would not replace existing mechanisms and tools,[147] but rather offer an additional possible path to access data. Although it might actually reduce legal certainty for companies potentially subject to conflicting obligations,[148] 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 complex[149] 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.

[145] See the proposed regulation Explanatory Memorandum, p. 1.

[146] Idem; also echoed in recital 8 of the proposed regulation.

[147] 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).

[148] Illustrating the focus on service providers' perspectives is recital 9 of the proposed regulation.

[149] 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".[150]

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.[151] 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".

The published proposal distinguishes two broad types of data: stored content data and 'non-content data', the latter comprising subscriber, access and transactional data.[152] 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 (Law Enforcement Data Protection Directive)".[153] Furthermore, a provision "recalls" that the regulation cannot alter fundamental rights obligations derived from Article 6 TEU.[154]

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

[150] Ibid., p. 14.

[151] See the judgment in *Big Brother Watch and Others*, op. cit., § 356.

[152] Recital 20 of the proposed regulation.

[153] Ibid., p. 3.

[154] Ibid., p. 13.

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".[155]

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.[156] As mentioned, EU data protection law does provide special rules for certain categories of data (generally designated as "sensitive data"),[157] 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.[158] 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.

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.[159] 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.

[155] Recital 21 of the proposed regulation.

[156] 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.

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

[158] Ibid., p. 22.

[159] Ibid.

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".[160] Yet there is no equivalent provision for European Preservation Orders, because presumably "the lesser interference with rights involved" would make that unnecessary.[161] 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 ones 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 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.

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 court or independent administrative body. In this regard, the

[160] Ibid., p. 20.

[161] Ibid.

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.[162]

## 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 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.

Contrarily to what is foreseen in the context of the EIO, under the proposed Regulation the competent judicial authorities of the country where the investigative measure should be executed would not have the possibility to ex ante assess and eventually non-recognise nor execute the execution of the order on the basis of 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 currently 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

[162] See the Judgment of the Court (Fifth Section) of 8 February 2018, *Case of Ben Faiza* v *France*, App. N § 75.

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.

Both the Commission's proposal on e-evidence and the CLOUD Act fail to ensure systematic cooperation among the competent judicial authorities in the countries concerned by a cross-border request for data. In the absence of such cooperation and without the systematic involvement of the competent judicial authorities 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[163]. Similarly, and with significant data protection implications, it must be highlighted the risk that would derive from changes in the Commission proposal which are 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.[164]

[163] Council 2018a, p. 10 and 22.
[164] 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. This definition does not encompass administrative authorities such as ministries or police authorities, which are "within the province of the executive". |
| 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. In some Member State, where prosecutors do not qualify as independent judicial authority and may be even considered part of the executive, LEAs could also include prosecutors. |
| 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 | |
|---|---|
| E-evidence proposals | 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:<br>• **Telecommunication services** (voice telephony, SMS and internet access services);<br>• **Internet-based services** enabling interpersonal communications such as voice-over-IP, instant messaging and web-based email services;[165] these also include over-the-top (OTT) communication service providers;[166]<br>• **Information society services** that store data for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;[167] 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<br>• **Internet infrastructure services**, such as IP address service providers and domain registrars, and associated privacy and proxy services (e.g. GoDaddy).<br>Small and medium enterprises also fall under the scope of the proposal. |
| Legal representative | 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. |

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

[166] 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.

[167] Ibid.

| Electronic information | | |
|---|---|---|
| Content data | The content exchanged by means of electronic communications services, such as text, voice, images and sound.[168] 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).[169] | |
| Non-content data | Metadata | 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.[170] Metadata also includes, for instance, data relative to the connection, traffic or location of the communication.[171] |
| | Subscriber data | Information that allows the identification of a subscriber to a service. Examples are the subscriber's name, address and telephone number.[172] |
| | Access logs | Information that records the time and date an individual accessed a service, and the IP address from which the service was accessed.[173] |
| | 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).[174] |

[168] 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).

[169] See Council of the European Union (2018b), p. 3.

[170] Ibid., Article 4(3)(c).

[171] See European Commission (2018a), p. 43.

[172] Ibid.

[173] Ibid.

[174] 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).

Bárd, P. and van Ballegooij, W. (2018), "Judicial Independence as a precondition for mutual trust? The CJEU in Minister for Justice and equality v. LM, New Journal of European Criminal Law", pp. 3-4 (https://journals.sagepub.com/doi/abs/10.1177/2032284418801569)

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).

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).

Carrera, S., Guild, E., Hernanz N. (2013), Europe's most wanted? Recalibrating Trust in the European Arrest Warrant System, CEPS Special Report No. 76/ March 2013 (https://www.files.ethz.ch/isn/162520/SR%20No%2076%20SC,%20EG%20&%20NH%20on%20the%20EAW%20.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.

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 Mistilegas (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).

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).

Janssens, C. (2013), "The Principle of Mutual Recognition in Criminal Law, Oxford Studies in EU Law".

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/).

Lenaerts, K. (2015) The Principle of Mutual Recognition in the Area of Freedom, Security and Justice, Paper presenter in the occasion of the Fourth Annual Sir Jeremy Lever Lecture All Souls College, University of Oxford, 30 January 2015 (https://www.law.ox.ac.uk/

sites/files/oxlaw/the_principle_of_mutual_recognition_in_the_area_of_freedom_judge_lenaerts.pdf)

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

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.

Sáenz Pérez, C. (2018), "Constitutional identity as a tool to improve defence rights in European criminal law", in *New Journal of European Criminal Law*, *9*(4), pp. 446–463.

Sellier, E. and Weyembergh, A. (2018), Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation, Study Requested by the European Parliament LIBE committee, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union PE 604.977 - August 2018.

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.

# ABOUT CEPS

Founded in Brussels in 1983, CEPS is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity and complemented by an extensive network of partner institutes throughout the world.

## Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process
- Provide a regular flow of authoritative publications offering policy analysis and recommendations

## Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals

## Programme Structure

### In-house Research Programmes

Economic and Finance
Regulation
Rights
Europe in the World
Energy and Climate Change
Institutions

### Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)
Energy Climate House (ECH)

### Research Networks organised by CEPS

European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)