CEPS Paper in LIBERTY and SECURITY in Europe

Access to Electronic Data for Criminal Investigations Purposes in the EU

Sergio Carrera and Marco Stefan

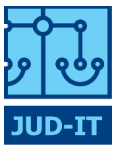
No. 2020-01, February 2020

Abstract

Within the EU and across the Atlantic, investigation and prosecution of crime increasingly relies on the possibility to access, collect and transfer electronic information and personal data held by private companies across borders. Cross-border access to and collection of data for the purpose of fighting crime raise several legal and jurisdictional issues. This paper comparatively examines the constitutional, legal and administrative frameworks on access to and use of digital information in cross-border criminal justice cooperation in a selection of EU member states. It presents key challenges in the application of the EU mutual recognition and mutual legal assistance instruments, as well as the existence of 'promising practices' across the EU and in transatlantic relations. The paper also assesses a set of legal and practical questions raised by the ongoing policy and normative debate on the so-called "E-Evidence" Package. Finally, it sets out a number of policy options and practical ways forward for EU and national policy makers to promote judicial cooperation for cross-border access to and collection of electronic data in line with EU and international rule law and fundamental rights standards.

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. The report takes into account developments occurred in the field of inquiry until the end September 2019.

Sergio Carrera is Senior Research Fellow and Head of the Justice and Home Affairs Section, CEPS, Brussels, Professor at the European University Institute (EUI), Migration Policy Centre, Florence, and Visiting Professor at Sciences Po, Paris. Marco Stefan is Research Fellow at the Justice and Home Affairs Section, CEPS, Brussels.



978-94-6138-762-2

Contents

List of Tables

1. Introduction

While working towards the establishment of an Area of Freedom, security and justice (AFSJ), the European Union (EU) has progressively developed a common criminal justice area that addresses different aspects of intra-EU and international cross-border judicial cooperation in criminal matters. These include investigative measures aimed at gathering evidence abroad for the purpose of investigating criminal activities.

The set of EU tools for criminal justice cooperation in the area of evidence gathering currently encompass the so-called 'European Investigation Order' (EIO) Directive 2014/41/EU, and Mutual Legal Assistance Treaties (MLAT) with countries like the United States (US). Both the EIO and the EU MLATs provide common supranational rules that also allows access to electronic data and the gathering of electronic information as evidence in criminal matters, in line with the fundamental rights and rule-of-law standards that govern the EU and member states' internal and external action.

Within the 'European Criminal Area', mutual recognition of judicial decisions - including those related to cross-border access to and gathering of electronic data in the context of criminal proceedings - relies upon the principle of mutual trust. The latter embodies a presumption that all EU Member States, and their respective judicial authorities, comply, uphold and safeguard the core EU constitutional principles laid down in Article 2 TEU, including the rule of law.

The principle of mutual recognition has been developed under the premise that EU member states cannot refuse the execution of EU criminal justice decisions on the basis of fundamental rights obligations enshrined in their national constitutions. The Court of Justice of the European Union (CJEU) has however also clarified that 'trust must be earned' (Mitsilegas, 2019). Mutual trust in the EU legal system cannot be considered as blind trust (Lenaerts, 2017). This certainly has been the message sent by constitutional courts in different EU countries such as Germany and Spain.

The CJEU has gradually revisited the 'automaticity' of mutual trust in EU criminal law. Member states judicial authorities have the duty to halt criminal justice cooperation under mutual recognition proceedings if there are reasons to believe that the execution of another EU country's decision would expose the individual concerned to a real risk of fundamental rights abuses.[1] In such cases, which represent exceptions to the principle of mutual trust, the executing member states' authorities are required to conduct an individualised assessment of the fundamental rights implications stemming from the enforcement of EU criminal justice decisions. Such fundamental rights considerations extend beyond non-derogable or absolute fundamental rights such as human dignity and the prohibition of torture and inhuman and degrading treatment enshrined in Article 4 of the EU Charter.

[1] See Case C-216/18 PPU *Minister for Justice and Equality v LM* (Deficiencies in the system of justice), Judgment of 25 July 2018.

The rights to an effective remedy and to fair trial (Article 47 of the EU Charter) have also been granted a cardinal importance in upholding the rule of law and the principle of effective legal protection enshrined in Article 19 TEU. The Luxembourg Court has found that effective judicial oversight constitutes *the very essence* of the rule of law, and concluded that its delivery crucially relies on independent courts of the EU member states. The importance to protect the rule of law by ensuring independence of the judiciary has been reinstated by all European institutions. This objective is now reflected in the EU inter-institutional policy setting and agenda, where the safeguarding of EU values included in Article 2 TEU stands as a key priority.

Independent judicial authorities play a key role in securing the rule of law, and their involvement is crucial to maintain trust and ensure the legitimacy of the European Criminal Justice Area, and of any instrument or agreement adopted in the name of fighting crime. Trust cannot be taken for granted, and enduring trust is a daily practice in the context of judicial cooperation in criminal matters. This also applies to measures, rules and practices directed at enabling access to electronic information in criminal investigations, which have profound impacts on the rights to fair trial as well as on the rights of individuals as data subjects.

An ever-close nexus exists between effective remedies, fair trial and the rights to privacy and data protection, as respectively enshrined in Articles 7 and 8 of the EU Charter. In a context where access to and preservation of electronic information and communications is playing an increasing role in criminal investigations, fair trials rights become increasingly interconnected and intimately dependent upon the respect of the rights of the 'data subject', as protected in the EU legal system.

As regards access to and subsequent use by law enforcement authorities of retained data, the Court of Luxembourg required that prior to access by the competent national agencies, the conditions of access must be reviewed:

> 'by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions'.[2]

Thus, access for law enforcement purposes to retained data held by private companies imperatively requires prior review varied out by a court or by an independent administrative body. Another manifestation of the key role played by independent oversight bodies in transnational data flows has emerged in the context of transfers of air passengers' data (PNR – Passenger Name Records) by airline companies to third states. In Opinion 1/15 of 26 July 2017 the Grand Chamber rejected the draft Agreement between the EU and Canada on the transfer of PNR data.[3] In such

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

[3] Opinion 1/15 of 26 July 2017, para 201.

occasion, the CJEU confirmed the need to ensure, except in cases of validly established urgency, that the conditions of access to information for the purpose of preventing, detecting, investigating and prosecuting crime are reviewed by a court or by an independent administrative body, such a national data protection authority (Mitsilegas and Vavoula, 2018).

Given the large volumes of personal data gathered and processed by private companies, and the transnational dimension of the internet, police and criminal justice policies increasingly focus on equipping investigating and prosecuting authorities with the possibility to access, collect and exchange electronic information held by private IT and telecommunication companies across borders. Since requests for data sought in the context of a criminal proceeding often have extraterritorial and cross-jurisdictional implications, strengthening judicial cooperation in criminal matters while preserving fundamental rights and the rule of law has become a key policy priority in the EU, as well as in cooperation with third countries. Well-functioning criminal justice cooperation instruments for cross-border evidence gathering are required to ensure that data are collected in ways which prevent conflicts among different legal systems and constitutional traditions, and ensure compliance with the EU Charter of Fundamental Rights (The EU Charter) and Article 2 of the Treaty on the European Union (TEU).

The JUD-IT project has comparatively examined the constitutional, legal and administrative frameworks on access to and use of digital information in cross-border criminal justice cooperation in a selection of EU member states. It has studied the main issues and challenges in the application of the EU mutual recognition and mutual legal assistance instruments as well as the existence of 'promising practices' across the EU and in transatlantic relations.

The priority given to access, preservation, production, collection and transfer of *electronic information and personal data* held by companies is raising a number of fundamental legal and practical questions to judicial and law enforcement practitioners, defence lawyers and the private sector both in the EU and across the Atlantic. The project aimed at gaining a better understanding of the main concerns and key issues from the perspective of each of these actors.

JUD-IT has sought to facilitate the identification of practical and policy ways forward for EU and national policy makers to promote judicial cooperation in criminal matters in a context of increasing use of electronic means and data in line with EU rule law and fundamental rights standards.

2. The European Investigation Order

KEY FINDINGS

- Through the application of the principle of mutual recognition to evidence gathering in criminal matters, the EIO allows different categories of electronic information to be accessed, collected and exchanged through direct cooperation among judicial authorities across borders.
- EIOs requiring collection of data allowing for the identification of persons holding a subscription of a specified phone number or IP address cannot lead to non-recognition or non-execution decisions based on the objection that such measures are not available in the state of execution. The executing authority might be required to execute, whenever practicable, provisional measures such as the preservation of data within a 24-hour deadline.
- Verifying the legality, necessity, and proportionality of data-gathering or preservation measures included in EIOs is the responsibility of the issuing member state's judicial authorities, which are responsible for performing the assessment against their own domestic legal standards, as well as in light of relevant EU primary and secondary law and the EU Charter. Issuing authorities are prohibited from using the EIO to collect evidence abroad that they are not able to obtain under their own domestic legal and constitutional procedures.
- The executing authority needs to follow the formalities and procedures expressly indicated by the issuing authority, but only to the extent that these are not contrary to fundamental safeguards provided under their own legal system. Execution of an EIO is supposed to take place in the same ways and under the same modalities (and related procedural safeguards) as if the investigative measure concerned had been ordered by an authority of the executing State.

The EU criminal justice toolbox encompasses a set of judicial cooperation instruments through which authorities in charge of investigating and prosecuting crime, as well as defence lawyers, can demand and obtain electronic information held by private companies in another jurisdiction.

When it comes to cross-border cooperation for evidence gathering within the EU criminal justice area, EU mutual legal assistance mechanisms are progressively being replaced by mutual recognition instruments.[4] The European Investigation Order (EIO) Directive[5] represents a key legal development in the field of EU judicial cooperation. It extends the application of the principle of mutual recognition to the cross-border gathering of evidence (also in digital form) in criminal matters. While the EIO does not expressly mention 'electronic evidence' as such, the inclusion of a reference to 'data' in the text of the Directive indicates that different categories of electronic

[4] One agreement between EU countries is still in place: The Convention on mutual assistance in criminal matters. Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the member states of the European Union, [2000] OJ C 197/1.

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

information can currently be collected and exchanged across borders through the use of this instrument.[6]

The EIO is based on a mediated model of judicial cooperation for cross-border evidence gathering (Carrera, González Fuster, Guild, and Mitsilegas 2015). Such model entails direct contacts and communication between pre-identified public bodies of the different countries concerned by a cross-border proceeding. Under the EIO, the judicial authorities in the issuing member state are those responsible to verify the legality, necessity, and proportionality of a cross-border decision.[7] Such assessment must be conducted by the competent authorities of the issuing country against their own domestic legal standards, as well as in light of relevant EU primary and secondary law and the EU Charter.

Member states authorities 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 allows for a shorter deadline when required by the seriousness of the offence or in other particularly urgent circumstances. The executing authority might for instance be required to execute, whenever practicable, provisional measures such as the preservation of data within a 24-hour deadline.[8] A double criminality check is maintained. This is so only for orders related to facts falling outside the list of the 32 offences for which double criminality has been abolished. These are offences which are not punishable in the issuing member state by a custodial sentence or a detention order for a maximum period of at least three years.[9] Such provisions ensure that double criminality grounds might only be raised by the competent authorities of the state of execution for certain categories of less serious offences. On the other hand, investigative measures requiring data allowing for the identification of persons holding a subscription of a specified phone number or IP are always available under the EIO, and cannot be refused in the country where the order is addressed based on the objection that such measures are not available in that legal system.[10]

The EIO system requires member states to cooperate in the field of cross-border evidence gathering based on minimum formality and speed, while at the same time imposing compliance with a set of key safeguards. Besides demanding participating EU countries to comply with the principle of mutual recognition of judicial decisions in criminal matters, the EIO includes a number of provisions directed at ensuring respect of the constitutional and criminal justice traditions of different member states, as well as EU fundamental rights and the rule of law standards.

[6] See Art. 13 of the EIO Directive. Recital 11 of the Directive also indicates that investigative measures under an EIO might 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".

[7] Art. 6(1)(a) of the EIO Directive.

[8] Art. 32(2) of t the EIO Directive.

[9] Art. 11(1)(g) of the EIO Directive.

[10] Art 10 (2) (e) and Art 11 (2) EIO.

The executing authorities need to follow the formalities and procedures expressly indicated by the issuing ones, but only to the extent that these are not contrary to fundamental principles provided under their own legal system.[11] Execution of another EU country's EIO is supposed to take place in the same ways and under the same modalities (and related procedural safeguards) as if the investigative measure concerned had been ordered by an authority of the executing State in an equivalent domestic case.[12] To ensure respect of such mechanism, it is thus important that issuing authorities specify whether an EIO is adopted during the pre-trial or trial phase of a criminal proceeding, because depending on the stage of the proceedings competent authority could be different in the executing country (e.g. EL; FR; HU; IT). Furthermore, the Directive requires the applicability of legal remedies equivalent to those applicable in a similar domestic case to the investigative measures indicated in the EIO.[13] While the substantive reasons for issuing the EIO may be challenged only in an action brought in the issuing State, this is without prejudice to the guarantees of fundamental rights in the executing State.[14]

An assessment to use an alternative investigative measure is also foreseen when the measure indicated in the EIO does not exist in the law of the executing country, or when the indicated measure is not available in a similar domestic case.[15] The introduction of specific provisions on comparable measures in the EIO is justified not only in light of wide range of investigative means covered by the Directive, but also because of the diversities of national measures and procedures to obtain evidence. At the same time, this rule does not apply as far as the investigative measures indicated in the EIO are considered as 'non-coercive' under the law of the executing State. As a general rule, the EIO establishes that recognition or execution orders requiring data allowing for the identification of persons holding a subscription of a specified phone number or IP address cannot be refused based on the objection that such measures are not available in the state of execution. The same applies to offences which are not punishable in the issuing member state by a custodial sentence or a detention order for a maximum period of at least three years, based on double criminality grounds.

By allowing the intervention of the competent authorities in both the issuing and executing country, the EIO ensures that every order is executed in accordance with the procedures and safeguards prescribed under the different legal systems concerned by the cross-border proceeding. On the one hand, the Directive includes provisions directed at preventing member states from obtaining evidence abroad that they are not able to obtain under their own domestic legal and constitutional procedures.[16] On the other hand, the executing authority might decide not

[11] Art. 9(2) of the EIO Directive.

[12] Art. 9(1) of the EIO Directive.

[13] Art. 14(1) of the EIO Directive.

[14] Art. 14(2) of the EIO Directive.

[15] Art. 10(1) (a) and (b) of the EIO Directive.

[16] Art. 6(1)(b) of the EIO Directive.

to recognise and/or execute an EIO when it has been issued for certain categories of (less serious) offences for which the requirement of dual criminality has not been met, or based on an assessment of the fundamental consequences that would derive from the execution of the measure requested in the EIO.

The EIO Directive list a number of specific non-recognition/execution grounds, which 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. It is also foreseen that hat the recognition or execution of an EIO 'may be refused in the executing State where there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter'.[17]

The possibility foreseen in this piece of EU legislation to refuse an EIO based on fundamental rights grounds implies that judicial authorities have a duty to verify whether the execution of an EIO is compliant with fundamental rights standards. Competent authorities are called upon to assess whether specific fundamental rights grounds of legitimate refusal to recognise and execute an EIO exist. 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). This non-recognition ground confirms that the presumption that all member states comply with fundamental rights is, in fact, rebuttable at all instances (Armada, 2015).[18] 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. Such way of cooperation allows avoiding conflicts of law and maintaining trust within the EU.

The EIO Directive also foresees that the executing authorities' role in reviewing fundamental rights might extent to the conditions for issuing an Order. Article 6(3) states that where "the executing authority has reason to believe that the conditions referred to in paragraph 1 [the issuing of the EIO is necessary and proportionate,[19] and the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case[20]] have not been met, it may consult the issuing authority on the importance of executing the EIO. After that consultation the issuing authority may decide to withdraw the EIO."

[17] Art. 11(1)(f).

[18] Instruments of mutual recognition in criminal matters adopted before the entry into force of the Lisbon Treaty only included a general reference to the Charter but did not include a specific ground for refusal in this regard.

[19] Art 6(1)(a).

[20] Art. 6(1)(b).

3. Implementing the EIO

KEY FINDINGS

- The EIO Directive only recently entered into force, and its timely transposition and implementation of the EIO represented an issue for some EU member states. More time is required for this instrument to fully flourish.
- The EIO scheme ensures mutual scrutiny over data requests through the involvement of competent judicial authorities (i.e. judges or prosecutors) in the issuing and executing country. The ex-ante involvement of judicial authorities for the purpose of issuing and executing orders might increase judicial oversight over data-gathering measures that, in a purely domestic context, could be adopted directly by law enforcement authorities (e.g. police officials).
- The EIO allows investigating and prosecuting authorities to cooperate between themselves with a significant degree of operational flexibility, also through the use of 'urgent procedures'. On the other hand, urgent requests for data only formally validated and issued by judicial authorities but substantially originating from police authorities result in some cases in a de facto 'shift' of decision-making from the judiciary to law enforcement agencies.
- When issuing EIOs, some member states lift the ex-ante court validation (from a judicial authority different from the one conducting the investigation) that would be necessary for the execution of equivalent measure in a purely domestic context. In such cases, EIOS are issued in a way which reduce guarantees otherwise applicable in purely domestic proceedings.
- Different treatments still apply to incoming EIO, when compared to equivalent domestic measures. Some member states impose one level of procedure in the form of centralized control by a central authority of EIO received by other EU member states. Such additional requirement is contrary to the principle according to which EIOs should be executed under the same procedures as if the investigative measure concerned had been ordered by an authority of the executing state. Furthermore, not all member states treat incoming EIOs with the same priority as domestic requests, and some EU countries appear to be unduly postponing their execution.
- The EIO system of cooperation is characterised by an imbalance between the powers of the prosecution and the defendant. The EIO Directive foresees the possibility for the suspected or accused person, or by a lawyer on his behalf, to request the issuing of EIOs in conformity with national criminal procedure. However, defence lawyers are often unaware of the possibility to request the issuing of EIO. In some cases, national law transposing the EIO does not include special provisions that an investigation order may be issued at the request of a suspect, accused or her/his defence counsel. The absence in national legislation of provisions allowing suspect or accused persons access to the EIO challenges the possibility to develop a positive defense, or to challenge the evidence of the prosecution.

- Due to the way in which criminal investigations are conducted by member states' authorities, investigative measures requested and executed through EIOs are often covered by 'secrecy', and suspects are only informed of access/use or transfer of their electronic data once the investigation is closed, just prior to the indictment.
- A set of practical challenges currently hamper the potentials of the EIO. These include the persistent lack of a streamlined approach followed by EU judicial authorities in the formulation and transmission of EIOs, as well as of specialised personnel and equipment in national administrations. With several member states still requiring EIOs to be issued or received in their own national language, translation also constitutes a recurrent delay factor.

The timely transposition and implementation of the EIO Directive has been an issue for some EU member states. A key finding from our research is that it is by now too early to conclude that the EIO is 'ineffective', slow or burdensome in practice. To date, such conclusions can neither be drawn with regard to the use of the EIO for accessing and exchanging electronic information sought for criminal justice purposes. JUD-IT research has instead showed that the implementation of the EIO in several EU member states has actually allowed for the introduction and operability of more 'flexible' procedures in comparison to previously existing instruments of judicial cooperation for evidence gathering in criminal matters. In countries where the EIO Directive suffered from transposition delays (e.g. LU), judicial actors and legal practitioners anticipate smoother cooperation with EU partners under EIO law, in particular thanks to the introduction of standardised form and tight time limits.

Judicial practitioners consulted in the JUD-IT project have underlined how, based on their experience, EIOs are swiftly and efficiently processed in practice and there are no major obstacles or structural deficiencies pertaining to the EIO model (e.g. BU; EL; IT). The EIO was referred to as the 'most mature' mutual recognition instrument applying to cross-border evidence-gathering in criminal matters, allowing for a significant degree of operational flexibility for judicial authorities, including the expedience and the uniformity that it has brought (AT; BU; EL).

The EIO allows for 'urgent procedures', as illustrated in several JUD-IT Country reports. For example, in Hungary, controlled deliveries or the application of covert investigations can be initiated by the competent director of the police or of the National Tax and Customs Administration, for a duration of 24 hours. The competent public prosecutor is immediately notified and will need to subsequently approve it. From the information provided by the European Judicial Network (EJN),[21] and JUD-IT research, email communication is permitted in some member states (e.g. EL, ES, FR), under the condition that it is then followed by the formal information.

[21] European Judicial Network (EJN, 2019), Competent authorities, languages accepted, urgent matters and scope of the EIO Directive1 of the instrument in the EU Member States, https://www.einforum.eu/cp/registry-files/3339/Competent-authorities-languages-accepted-scope-26-August-2019.pdf.

English language is accepted in some member states (BU, HU, EL, NL). Some countries (e.g. LU) accepts EIO in multiple languages (i.e. French, German, English).

The systematic *ex-ante* involvement of judicial authorities[22] for the purpose of issuing and executing EIOs introduces a minimum level of judicial oversight over data-gathering measures that, in a purely domestic context, could be adopted directly by law enforcement authorities. In some member states (AT, DE, FR, HU) the EIO showed in fact a potential to increase the level of judicial scrutiny and protection over the issuing and execution of cross-border data-gathering measures.

At the same time, the JUD-IT country reports made it possible to identify a number of gaps and examples of incorrect national implementation that call for close scrutiny and action. An especially problematic aspect in this regard concerns the issuing of the EIO by some EU countries in ways which lowers domestic standards on judicial checks and balances. According to the text of the EIO Directive, member states authorities should not use it as 'forum shopping' and obtain 'evidence' abroad while evading domestic checks and balances and procedures. And yet, it appears that the judicial validation required at the domestic level for data requests might be eluded in EIO cross-border situations (FR; NL; LU)

In France, for instance, prior authorisation by a judge of liberty and detention is required in cases when the prosecutor or the investigating judge intend to perform a search of computer system during the preliminary investigations, and such measure is to be performed without the consent of the person concerned.[23] However, if the execution of such measure is requested through an EIO transmitted to another EU country, the French prosecutor or the investigating magistrate are not obliged to obtain such authorisations at the domestic level, but can simply indicate in the EIO that the investigative acts requested therein can only be executed by the executing State with the prior authorisation of a judge, and in line with the manner and timings foreseen by the French *Code de Procedure Penal* (CPP). There is however no real guarantee that such a prior authorisation by a judge will be effectively ensured in the country of execution. Other countries like Sweden have correctly implemented the EIO in this respect, by envisaging that an EIO may only be issued if the conditions applying to conducting the investigation during a Swedish domestic investigation or trial in criminal proceedings and law are actually met (SE).

In some countries (e.g. EL) urgency of requests for data is used in practice to operate a 'shifting' of the decision-making power from the judiciary to law enforcement agencies. This practice is liable to lead to manipulation of prosecutors/judges, who are often apprised of limited aspects of the case and almost automatically validate data requests made by the police. This practice becomes

[22] These authorities might be both judges and prosecutors, depending on various factors including for instance the crime involved, the type of data sought, the nature of the measure to be executed through the EIO, as well as the stage of proceedings.

[23] Article 76 para 4 of the French Code of Criminal Procedure.

all the more concerning in the EIO context, considering that any data lawfully obtained based on urgency procedures shall be subject to be handed over pursuant to judicial cooperation duties.

In Luxembourg, the implementation of the EIO means that one level of procedure in the form of centralised control of outgoing requests for *entraide* or orders is stripped away. While this is justified in light of the 'minimum formality requirement', problems arise from the fact that the country maintained a systematic review of incoming EIOs in the execution phase, contrary to the principle according to which EIOs should be executed under the same ways as if the investigative measure concerned had been ordered by an authority of the executing State.

A cross-cutting finding from the JUD-IT research is that the EIO system of cooperation is characterised by an imbalance between the powers of the prosecution and the defendant. Ultimately, even if Article 1(3) EIO Directive foresees the possibility for the defendant to request the competent prosecutor/or court to issue an EIO, this appears to be rarely possible in the domestic systems analysed. JUD-IT research has brought light to the fact that defence access to this mutual recognition instrument is very limited in practice. In some cases, the EIO implementing national law has not included any special provision that an investigation order may be issued at the request of a suspect, accused or her/his defence counsel (SE). While the Directive foresees that defence requests directed at obtaining the issuing of EIOs can be enabled through reference to domestic laws regulating criminal procedure, there are uneven national rules and blurred/obscure administrative practices regarding when and if suspects can demand such measures, or have access to the data gathered for purposes of criminal investigations. JUD-IT research has showed that even when such possibility exist, legal practitioners are often not aware of it (HU). Moreover, in some EU countries a large margin of discretion is left to the judicial authorities responsible for receiving, assessing and validating defence's request for issuing an EIO (e.g. ES; HU).

The effectiveness of existing remedies and in particular the possibility for suspects/data subjects to challenge EIOs in the issuing state has been by and large considered inadequate. Very often, investigative measures are covered by 'secrecy' and suspects are not informed or aware of access/use or transfer of their electronic data. Suspects often become aware of such measures only after the investigation closure and just prior the indictment, with defence lawyers expressing complaints about late or non-notification (ES; HU; EL; SE). In some EU member states access to files by the suspects representatives only happens right before the court procedures (HU).

The existence of other data-gathering instruments (e.g. Council of Europe Budapest Convention) that can be used in parallel to the EIO was perceived positive by some practitioners who consider it important to have different tools that could be combined (ES; EL; FR). However, it was also underlined as one possible cause of underuse of EIOs and inefficiency as well as a risk of forum shopping. Such risks could emerge in particular where the international cooperation tools offered by the Budapest Convention are used in ways which might in some cases lower down EU rule of law or fundamental rights protection standards otherwise applicable to cross-border cooperation

under the EIO.[24] Other practical issues may relate to the choice of proper instrument investigative instrument and procedure, identification of relevant contact points, as well as the correlation/equivalence of legal terms and notions across EU member states (ES; BU).

JUD-IT research has showed how direct (formal and informal) contacts and interactions with their colleagues across borders and throughout different phases of EIO procedures constitute an important part of their daily work. Such practices of cross-border 'judicial dialogues' currently allows competent judicial authorities in member states to exchange evidence requested through standardised forms across borders, and through trusted channels and means of communications. They also allow executing authorities to require the issuing ones to provide any additional information, adjustments and/or rectifications that might be necessary in order to lawfully execute the requested data-disclosure measure.

An example provided in this respect is represented by a case where prosecuting authorities from two EU countries (reportedly BU, and AT) have asked their counterparts in another member state (i.e. Italy) to take the lead in the investigation of a specific fact that (under the national law of the requesting member state) did not meet the serious crime threshold (5 years) required to proceed.[25] In all the examples mentioned above, cooperation was made possible through contacts and cooperation among judicial authorities of the different member states concerned.

Prosecutors, judges and defence lawyers who were consulted and interviewed during the project agreed that while the EIOs has already shown its potentials as judicial cooperation instruments for cross-border evidence-gathering, more time and efforts are needed in order to allow it to 'flourish' fully. It was for instance mentioned that not all member states treat incoming EIOs with the same priority as domestic requests, and that some EU countries appear to be unduly postponing their execution.

The current absence of a streamlined and uniform approach to be followed by EU judicial authorities in the formulation and transmission of EIOs has been also identified as an obstacle, as well as the lack of specialised personnel and equipment in national administrations of justice (EL). Translation seems to be a recurrent issue highlighted by judicial authorities whose experiences in dealing with this instrument have been gathered through JUD-IT qualitative research (BU; EL; IT).

[24] See for instance the possibility offered by Art. 32.b of the Council of Europe Budapest Convention, according to which a part may 'without consent of the another Party, access of receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party though that computer system'.

[25] In countries such as Bulgaria, metadata (and in particular traffic data) is only accessible for serious crime (that is, crime as capable of attracting a custodial sentence of more than 5 years). Requests for data sought for the prosecution of non-serious crime would thus be considered unlawful according to the law of that country. For instance, it was observed that 'computer crime' is not considered 'serious crime' according to Bulgarian law. This category of crime does not meet the 5 years custodial sentencing threshold which allow prosecuting authorities to lawfully access certain categories of data, including metadata.

Some member states have adopted a strategy to tackle such practical issues. A 'promising practice' was found in Bulgaria, where every District Prosecution Office awards a contract (following a public tender) to a private translation firm, which releases the Office from this burden, accelerates the process and ensures proper legal translation. Bulgaria also accepts EIO requests in English.

The positive role and contributions ensured by the European Judicial Network (EJN) and Eurojust (in particular by financially and practically supporting Joint Investigation Teams, JITs, in cases where they are consulted) have been highlighted as clear examples of facilitating efficient cooperation by providing contact points and information and communication platforms, liaising with relevant authorities, and providing training activities and materials (e.g. SE). Initiatives that practitioners consulted and interviewed during JUD-IT research described as particularly promising in order to resolve practical issues related to EIOs formulation and transmission consist of the creation of an electronic (and user-friendly) version of the EIO, and the establishment of a platform for the secure exchange of evidence in digital form (using the electronic evidence digital exchange platform as a tool for the secure transmission of data) that can guarantee the validity, integrity and authenticity of the requests, but also speed up the process through which competent authorities reply and transfer electronic information.[26]

[26] The e-CODEX (e-Justice Communication via Online Data Exchange) is a project co-funded by the EU and developed by a large consortium including 22 Ministries of Justice or their representatives as a part of the European e-Justice Digital Service Infrastructure.

4. Member state laws and practices on access to electronic information

KEY FINDINGS

- National legislation related to investigative measures directed at preserving, accessing and collecting electronic information held by private companies and sought during criminal proceedings varies significantly from member state to member state.
- The authorities responsible for requesting, validating, and executing investigative measures targeting electronic information differ depending on factors such as the specific type of data sought, whether the measure involves preservation or production of data, but also based on the categories of persons affected, as well as the specific stage of the proceeding in which such measures are to be executed.
- *Ex ante* independent judicial oversight and validation of domestic and/or foreign requests for different categories of data sought for criminal justice purposes is often required by member states' legislation aimed at preventing unauthorised intrusions of fundamental rights and/or sovereign interests protected at the constitutional level. In some EU countries, for instance Belgium, Bulgaria, France, Germany, Greece, Luxembourg and Spain, *ex-ante* validation by a court is under certain circumstances required in order to lawfully obtain the preservation or production of subscriber and/or access data.
- A constant feature is that access to data (including non-content) sought by investigating and prosecuting authorities in the context of a cross-border criminal proceeding can only be authorised by a domestic judicial authority of the country where the measure has to be executed. Under national legislation, providers of IT and telecommunication services are not allowed to respond to direct requests for data issued by foreign investigating and prosecuting authorities.

While across the EU access to data for criminal justice purposes is considered a fundamental right sensitive measure, the substantive rules and procedural safeguards applying to investigating and prosecuting authorities' requests for electronic information vary from one member state to another (Sieber and von Zur Mühlen, 2016).

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 and practices. For instance, in certain EU countries covered by the JUD-IT research (ES), access to data including non-content data (e.g. IMSEI and IMEI codes) has until recently been limited to the investigation and prosecution of 'serious crime'. In some other member states, the seriousness of crime determines the authority responsible for validating a request for data sought for criminal justice purposes. In France, for instance, the involvement of an independent judicial authority is required for certain categories of serious crime, regardless of the type of data sought by the investigative measure. At the same time, the concept of serious crime assumes different meanings in specific national legal systems, and currently it still lacks a definition under EU law. Among the EU member states covered

by the JUD-IT research, only some have specific legislation on the admissibility of data as evidence in criminal proceedings (e.g. HU). Other member states do not count on such a legal framework being in place, and just make use of general legislation dealing with "documents" (e.g. ES; IT; LU) or "physical evidence" (DE).

National legislation also outlines the procedural rules and identifies the oversight mechanisms that apply to the issuing and execution of both, domestic and cross-border requests for data sought for the purpose of preventing, detecting, investigating and prosecuting crime. The authorities responsible for requesting, validating, and executing investigative measures targeting electronic information differ depending on factors including not only the crime being investigated or prosecuted, but also the specific type of data sought, whether the measure involves preservation or production of data, but also based on the categories of persons affected, as well as the specific stage of the proceeding in which such measures are to be executed.

Ex-ante independent judicial oversight and validation of domestic and/or foreign requests for data sought for criminal justice purposes is often required by member states' legislation aimed at preventing unauthorised intrusions of fundamental rights and/or sovereign interests protected at the constitutional level.[27] In countries belonging to the continental prosecutorial system, the investigative judge plays a crucial role, including that of 'validation', during the trial phase (EL; HU; BU). The JUD-IT country reports also show that in some of the EU member states examined the involvement or validation by an independent judge takes place, regardless of the stage of the proceeding, when there are fundamental rights considerations involved in the request for electronic information (e.g. ES; HU). However, a key challenge identified is that a rigorous scrutiny by independent judicial authorities may be difficult to ensure in practice (FR; EL).

In some member states, validation by an investigative judge or a court during specific phases of the pre-trial or trial criminal procedures is required for different categories of non-content data, including in some cases access data and subscriber information (ES). In other countries, an *ex-ante* validation by a judge is required when requests are to be executed without the consent of the person concerned and regard the preservation of data sought during search and seizure operations for *'délits flagrants'* or in preliminary investigations (FR), or depending on the degree of coercion, i.e. investigative measures requiring coercive measures (LU; ES). Different countries require judicial validation or a prior court order for coercive measures entailing access to and seizure of stored communications (DE; ES; SE). In some of the member states studied (LU), a lack of agreement emerged between stakeholders involved as to whether the kind of data sought (e.g. content or non-content data) is relevant and have consequences for the type of fundamental rights protections and safeguards accorded.

[27] Judgment of the Court (Fourth Section) of 24 April 2018, *Case of Benedik v. Slovenia,* App. No. 62357/14.

The criteria used to determine the authorities competent to assert criminal jurisdiction also vary significantly across the countries covered by the JUD-IT research, with some member state looking at the place where services are offered (BE; ES), the place where provider/company is established (BU; SE), or where the criminal offence has occurred (LU). A key issue highlighted with regard to 'cloud service providers' relates to the fact that thy use servers all over the world, which makes it difficult to locate where the data requested actually is, or where the measure has to be executed (SE). In several EU countries (e.g. BU; HU; ES), national authorities are in some cases and under certain conditions allowed to order disclosure of data regardless of where the latter is stored. While legally adopted under the law of the issuing country, such measures often have cross-jurisdictional implications, and might result in conflicts with another country's law.

A constant feature that emerges from the JUD-IT research at the national level is that access to data (including non-content) sought by investigating and prosecuting authorities in the context of a cross-border criminal proceeding can only be authorised by a domestic judicial authority of the country where such a measure has to be executed. Under member state's national legislation providers of IT and telecommunication services are not allowed to respond to direct requests for data issued by foreign investigating and prosecuting authorities.

When it comes to cross-border requests for data issued by EU investigating and prosecuting authorities and addressed directly to private companies, cooperation remain, to date, largely "voluntary". Voluntary means that "there is a domestic legal measure which cannot be enforced directly in the recipient country. Nevertheless, the distinction between voluntary and mandatory cooperation is not always easy to establish, and in fact, in the absence of a clear legal framework the parties involved may disagree on the voluntary or mandatory nature of the direct cooperation".[28]

Through the involvement of competent judicial authorities in the state of execution, the EIO Directive allows for data gathering measuring measures issued in another EU country to be domesticated and legally enforced. As outlined in Section 2 of this Report, the rules and procedures for judicial cooperation incorporated in the EIO already allow *electronic data* collected as part of a cross-border criminal investigation, and during the pre-trial of a proceeding, effectively qualify as *evidence* accepted as 'admissible' before a court of law.

This is particularly important in a context where rules on admissibility of evidence in criminal proceedings vary across the Union. While it appears that in some EU countries (e.g. BE) data collected according to the wrong procedure or unlawfully in the pre-trial phase could still be

[28] European Commission (2018), "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, p. 26, footnote 37.

admitted as 'evidence' depending on the judge's discretion, this is not the case in others. Some member states (e.g. BU; DE; ES; FR) have stricter exclusionary rules according to which the evidence that has been, either directly or indirectly, collected in infringement of fundamental rights and without the required ex ante judicial authorisation would be declared inadmissible by the Court.

Table 1. EIO and requests for data - Comparative Table

MS	Issuing and/or executing EIO imposes judicial validation not required in domestic context[29]	Implementation practices leading to potential breach of EIO principles and rules[30]	Prosecutors can issue requests during pre-trial phases (no prior validation by a court)	Prior court validation required for accessing content data under national law	Prior court validation required for non-content data (incl. subscriber and access) under national law	Prior court validation expressly required for preservation of data under national law	Access to data only for prosecution/ investigation of serious crime	Central authorities involved in the EIO process	Defence faces challenges in participating in EIO process	Data inadmissible as evidence if collected in violation of FR	Constitutional issues[31]
AT	✓		(✓)						✓	n.a.	
BE			(✓)	(✓)	(✓)				n.a.	(✓)	
BU				✓	✓	✓	✓	(✓)	n.a.		
DE	(✓)		✓	(✓)	(✓)		✓		✓	(✓)	✓
FR	✓	(✓)	(✓)	(✓)	(✓)	(✓)		(✓)	n.a.	(✓)	
EL		(✓)	✓	(✓)	(✓)	(✓)			(✓)	✓	
ES		(✓)	(✓)	✓	(✓)		✓		✓	✓	✓
HU	✓	✓							✓	n.a.	
IT	(✓)	✓	✓	(✓)					✓	✓	(✓)
LU		(✓)	(✓)	(✓)	(✓)	(✓)	n.a.		(✓)	n.a.	
NL			✓	✓				✓	✓		
SE			✓	(✓)	(✓)	(✓)	n.a.	(✓)	✓		✓

Y: Yes *(Y): Yes, depending on specific circumstances* *n.a.: Information not available*

Source: JUD-IT Country Reports.

[29] Including from prosecutors, whereas in domestic cases requests can be made directly by the police. Also includes cases where domestic measure may be issued by a prosecutor, but EIO needs to be validated by a judge/court.

[30] EIO implementation lead to lowering of procedural safeguards provided under national law for issuing request for data, against EIO provision.

[31] National authorities and/or constitutional courts raised doubts as to the constitutionality of implementing mutual recognition instruments when this undermines or runs counter constitutional safeguard provided at the national level.

5. The EU-US Mutual Legal Assistance Treaty

KEY FINDINGS

- JUD-IT research has not confirmed that MLATs are by design ineffective tools for handling cross-border access to data. The JUD-IT research has instead shown that the current lack of resources and specialized personnel, both from the EU and US side represent a critical factor behind the length of time required for evidence gathering in the scope of EU-US MLAT. EU judicial authorities suffer from an insufficient understanding of US rules (probable cause) applying to access to data for criminal justice purposes. Only a few member states have appointed specialised liaison magistrates in the US.
- Recent initiatives such as the "MLAT Reform" program show that significant improvements to practical cooperation under MLAT procedures are possible. The Office for International Affairs at the DoJ is understaffed, underfinance, uses a 1998 case management software, there is currently no online platform for incoming requests from foreign governments. The US also lacks specialised judicial bodies working especially on foreign request. Initiatives such as the "MLAT Reform" program (through which the US Department of Justice managed to reduce the amount of pending cases by a third) show that significant improvements to practical cooperation under MLAT procedures are possible. More financial and human resources and support would be needed to ensure efficient MLATs implementation.
- By subjecting cross-border requests for data to mutual and systematic judicial scrutiny, the EU-US Mutual Legal Assistance (MLA) Agreement gives the competent judicial authorities of each of the parties concerned the possibility to effectively review the data-gathering measure issued by the other one. From an EU law perspective, several questions arise regarding 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. Outside the scope of the EU-US MLAT, the GDPR restricts the transfers and disclosures of EU data to a set of pre-defined exceptional circumstances.

As far as cross-border demands for electronic information involving EU member states which are not part to the EIO Directive (i.e. Ireland or Denmark), or third countries (e.g. the US or Japan), EU Mutual Legal Assistance Treaties (MLATs) provide channels for requesting, gathering and exchanging data for criminal justice purposes.

The exact ways in which MLA requests are issued and processed largely depends on the specific MLA instrument used to enact cooperation, as well as on the constitutional tradition and relevant legal and institutional framework of the countries concerned (Galli, 2018). Despite the differences in national systems and procedures applying to MLA requests, two constant features traditionally characterise the process: first, the receipt and assessment of the request for access by the

designated authority of the requested state in charge of examining the MLA request against existing domestic and supranational legal requirements and standards; and second, the involvement of judicial authorities which are respectively competent, under national law, for validating and executing the requests for data. During the second step, the designated authority transmits the request to the prosecutor's office to obtain a court order. In the scope of MLATs, EU member states' political bodies (e.g. Ministries of Justice acting as central authorities) and judicial actors (including, depending on the country, courts and prosecutors) are involved in supervising and examining cross-border requests, although there are some MLA conventions that allow for direct cooperation between judicial authorities.

As for transatlantic cooperation, the EU–US MLA Agreement[32] complements existing bilateral treaties with particular member states and amends some of their provisions, if they provide for less effective avenues of cooperation between EU member states and the US.[33] For member states that do not yet have an agreement with the US, the EU–US MLA Agreement may provide a suitable legal basis for cooperation.

A consistent feature of EU-US cooperation in the field of evidence gathering under the existing MLA framework 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 both the issuing and requested country (Carrera at al., 2015. pp. 7-8). The involvement of independent judicial scrutiny in the country where an MLA request is addressed guarantees that each request for data is carefully assessed. EU law enforcement requests for access to data stored in the US are assessed against the so-called probable cause standard, as enshrined in the Fourth Amendment to the US Constitution. In turn, member states judicial scrutiny over US requests for data channeled through transatlantic MLA agreements is designed to ensure that the rights of suspects and accused person, as well as those of concerned third parties and data subjects are duly protected in line with EU and national criminal justice and data protection standards.

JUD-IT research has not confirmed that MLATs are by design ineffective tools when handling international cross-border requests for data in a transatlantic context. The JUD-IT research has instead shown that the current lack of technical resources and specialized personnel, both from the EU and US side, represent a critical factor behind the length of time required for evidence gathering in the scope of EU-US MLAT. Expert discussions held throughout the JUD-IT project revealed that the Office of International Affairs (OIA) at the US Department of Justice (DoJ) is understaffed (lacking specialised judicial bodies working especially on foreign requests), and

[32] Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America.

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

underfinanced. The DoJ can furthermore only count on outdated information processing tools. It was mentioned that the OIA still uses a 1998 case-management software and lacks an online platform for incoming requests from foreign governments.

Such findings confirm previous analysis which already suggested the US Congress to adopt legislation allowing the Department of Justice to create an online submission process for MLAT requests on the DOJ's website, improving how these requests are submitted and tracked (McQuinn and Castro, 2017).[34] Additionally, there is no publicly available guidance nor exhaustive information on the OIA's website on how to submit a successful MLA request, and on how to comply with the probable cause standard.

Insufficient judicial training on the EU side has been referred to as a major obstacle towards ensuring that requests originating from member states' judicial authorities take due account of US legal standards, and most notably that regarding the probable cause. Other identified issues include the correct application of dual criminality, in particular regarding the US constitutional right of freedom of expression (ES; HU); and difficulties in proving or substantiating 'urgency', e.g. the existence of a clear and imminent threat against specific people (ES). Further causes of delays identified by practitioners and regarding requests issued by EU authorities include misunderstandings regarding the procedures, and translation issues (IE); as well as the lack of knowledge of the exact location of the electronic data (ES; SE). As far as data requests originating from the US are concerned, practical and legal obstacles on MLATs implementation reportedly include a lack of clarity in the ways in which the requests are formulated (ES).

Practitioners interviewed and consulted during the JUD-IT research and activities in the EU and the US highlighted that more financial and human resources and support would be needed to increase efficiency in MLATs implementation. They suggested an online network with all relevant information and allowing for submission of requests 24 hours a day and seven days a week, including information on follow up procedures and expected timetable (e.g. BU). Others highlighted that an official chart/explanation of the various stages comprising the investigation in different member states and the legal protections/safeguards applicable in each of them would be of great assistance (IE). Recent EU initiatives directed at increasing funding towards training for practitioners, including most notably on probable cause requirements, appears particularly valuable tool to improve criminal justice cooperation in the field of data-gathering at the transatlantic level.

On the US side, initiatives such as the "MLAT Reform" program undertaken by the US Department of Justice (DoJ) reportedly allowed to reduce the OIA caseload backlog by a third, 'from an all-time high in 2016 of 13,421 to less than 9,038' in 2019. Such results were obtained through the

[34] These scholars also recommended Congress to allow the DOJ to create an online docketing system for all MLAT requests that could allow foreign governments to track the status of their requests, improving the overall transparency of the system.

disbursement of 13 million dollars and the opening of 72 positions (37 attorneys and 35 paralegals) at the DoJ Office of International Affairs (OIA).[35] While not exclusively limited to incoming requests, and not exclusively tackling issues related to the gathering of electronic data, the MLATs reform shows that significant improvements to practical cooperation under MLAT procedures are possible, provided that adequate financial and human resources are deployed. Such resources could be used by the OIA to support prosecutors and law enforcement in the US and abroad in navigating domestic and foreign laws, treaties, and other requirements. The DoJ also recognised that 'to continue the progress made, permanent funds are needed to cover these critical positions and to allow the US government to sustain a 'timely and efficient international framework for allowing foreign governments to request access to data stored within the United States'.[36]

Other solutions currently explored to improve cooperation between member states and US judicial and diplomatic authorities include the organization 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. Simplifying procedures could also help reducing processing times of incoming data requests issued by EU authorities and executed by the US through existing MLA channels. It has been noted that currently, "DOJ reviews all data it receives from companies pursuant to an MLAT request before forwarding that data to the requesting government. However, because both DOJ and the U.S. Attorney's office have already cleared this request before serving it on the company, this step is unnecessary" (Mcquinn and Castro, 2017).

Outside MLA channels, EU investigating authorities may address requests for certain categories of electronic information, and most notably non-content data, directly to US service providers. To date, this form of direct cooperation with US service providers remains however largely voluntary in nature. US law in fact only allows, but not oblige, US service providers to disclose non-content data to foreign authorities. As a consequence, data disclosure requests addressed directly to service providers lack legal certainty, especially when compared with MLA regimes, under which incoming foreign requests are to be executed (as if they were domestic ones) by virtue of a compulsory order issued by the competent judicial authority in the country of execution. And yet, noting that requests to access and gather electronic information held by service providers across borders have become a common criminal investigative practice across the EU, the Commission expressed doubts that current and future volumes of data requests could be dealt with under MLA processes.[37]

[35] United States, Department of Justice, "FY 2019 Budget Request: Other Key Increases".

[36] Ibid, p. 1.

[37] European Commission (2018), "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

Figures provided in the so-called 'transparency reports' produced by tech companies such as Facebook, Google, Microsoft, Twitter and Apple indicate a constant increase in data requests received by these US service providers. The European Commission's estimated that, given the current market share of these companies, "up to 90% of current cross-border requests for non-content data are sent to these five providers".[38] While indicating that these requests "mostly" concern non-content data, the Commission also noted how these transparency reports suffer from important limitations. For instance, the reports do not distinguish whether reported requests came directly from the member state in which they originated, or from an authority which mediated such request. As such, based on the information provided by the transparency reports it is difficult to precisely quantify the amount of requests executed based on voluntary (unmediated) disclosure procedures, compared to those executed through MLA cooperation mechanisms.

A particular set of challenges emerge when data-gathering measures addressed directly to service providers subject to EU law originate from non-EU countries, including the US. US investigating and prosecuting authorities can in fact directly order US companies to produce data stored aboard, including when such data are in the EU, or fall under the scope of EU data protection legislation. If probable cause is shown, the US government can in fact obtain a warrant under the Stored Communication Act (SCA) requiring an Internet Service Provider to produce customer information, emails, and other materials, regardless of their location. The power to order disclosure of data stored overseas was traditionally justified on the basis of the special nature of SCA warrants, and the understanding that it is for the US company with control over the data to grant US authorities the power to compel its production (Kyriakides, 2014).

After the authority of US federal courts to issue warrants for the search and seizure of data located outside the territory of the United States was challenged in the *Microsoft Ireland* case,[39] the US government introduced the CLOUD Act,[40] which the US legislator adopted with the intention of clarifying that the SCA's scope of application extends to data stored abroad. Part I of the Act[41] now formally grants US authorities the power, under US law, 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

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 2018, p. 9.

[38] Ibid., p. 14.

[39] The dispute essentially questioned the lawfulness of extraterritorial assertion of US criminal jurisdiction in light of standing (i.e. pre-CLOUD Act) domestic legislation. The US Department of Justice argued that its warrant authority under the SCA required US-based companies to turn over the requested data, regardless of where the latter were stored. Microsoft, by contrast, defended that this authority did not extend to data located outside United States territory.

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

[41] Section 103 of the CLOUD Act.

also be ordered to preserve data in their possession for up to 180 days prior to the issuance of any compulsory process.

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. An especially controversial point seems to be whether articles 48 and 49 of the EU General Data Protection Regulation (GDPR) authorise, or rather impede, the disclosure and transfer of data requested by US law enforcement authorities according to Part I of the CLOUD Act.

Prima facie, Article 48[42] of the GDPR seems to forbid controllers or processors falling under EU jurisdiction to transfer or disclose personal data to third (i.e. non-EEA) countries' authorities when such data have been requested outside the legal channels provided by existing MLA agreements. In light of this provision, many companies might be reluctant to directly execute a US warrant, given the risk that compliance with such a measure could entail breaching EU data protection law, and expose them to a fine for up to €20 million or, in the case of a company, 4% of the worldwide annual turnover. On the other hand, some speakers and participants who took part in the JUD-IT Task Force noted that Article 48 of the GDPR was purposely formulated in an ambiguous way.[43] On the one hand, the article stresses that third countries authorities' requests for transfers or disclosure of data "may only be recognised or enforceable" if based on an international agreement (i.e. an MLA). On the other hand, it also appears to contradict itself by indicating that this is "without prejudice to other grounds for transfer" pursuant to the same Chapter of the GDPR. In this regard, it was noted that a reference to "derogations" for specific situations (including "important reasons of public interests") is included in the text of Article 49 of the same Regulation. According to some, this provision could thus allow direct cooperation between EU service providers and US law enforcement authorities.

During the last meeting of the JUD-IT Task Force, one speaker noted that (although included in Chapter 5 of the GDPR) Article 48 *per se* cannot constitute a legal basis for disclosure nor transfer. Data can in fact well cross borders while still remaining under the scope of the GDPR. Rather than authorising disclosure or transfer of data, Article 48 of the GDPR seems instead to require that transfers and disclosures of EU data to third countries' authorities comply with the set of rules and standards provided under primary and secondary EU privacy and data protection law, as

[42] 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."

[43] Early drafts of the Regulation expressly foresee a ban on transfers to foreign regulators to disclose and transfer data to foreign authorities without specific prior approval of a domestic data protection authority. The provision proposed during the negotiation of the GDPR has however been taken out of the final text.

progressively interpreted by the CJEU. These EU legal requirements must be met in order for a service provider subject to the GDPR to lawfully execute a cross-border data request under EU law.

The question that remains to be answered, therefore, is whether and how respect of such conditions can be ensured effectively in a legal and operative context such as the one established by Part I of the CLOUD Act.[44] 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.[45] 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 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.[46]

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. Outside the MLA channels, the scope that service providers subject to EU law have to lawfully execute US authorities request for data is limited to exceptional circumstances which are precisely enumerated and circumscribed in the GDPR.[47]

By subjecting cross-border requests for data to mutual and systematic judicial scrutiny, the EU-US MLA Agreement gives the competent judicial authorities of each of the parties concerned the possibility to effectively review the data-gathering measure issued by the other one. The importance of planning for systematic and reciprocal judicial oversight over EU-US cooperation in

[44] Part I of the 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".

[45] 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.

[46] 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.

[47] EDPB/EDPS (2019), Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence, 10 July 2019.

the field of evidence gathering was highlighted by the European Data Protection Supervisor (EDPS) in its Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence. The EDPS recommended in particular the involvement of judicial authorities designated by the other Party to the agreement as early as possible in the process of gathering electronic evidence so that these authorities would have the possibility to review the compliance of the orders with fundamental rights and raise grounds for refusal. [48]

The European Data Protection Board has stressed that: "In situations where there is an international agreement such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to an existing mutual legal assistance treaty or agreement".[49] Jointly with the EDPS, the Board has recently reiterated that "where disclosure of personal data is compelled by a third-country authority, the MLAT process must ensure that data is disclosed in compliance with EU law, and under the supervision of the courts in the EU".[50]

[48] EDPS (2019), Opinion of the European Data Protection Supervisor on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence, 2 April 2019.

[49] EDPB (2018), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, p. 5.

[50] EDPB/EDPS (2019), p. 3.

6. The e-evidence proposals

KEY FINDINGS

- The Commission proposal for a regulation on European Production and Preservation Orders envisages the introduction of two new crime-fighting tools that would allow EU member states investigating and prosecuting authorities to compel service providers by sending the respective Certificates (European Production Order Certificate – EPOC and European Preservation Order Certificate – EPOC-PR) across borders to produce or preserve electronic information sought in the context of a criminal proceeding. The company or its legal representative would be responsible for receiving and enforcing the European Production and Preservation Orders.

- Different judicial authorities would be responsible for issuing the orders depending on the type of measure concerned, and data sought. Prior validation by a court would be required for production orders concerning content and traffic data. These data could be requested for offences capable of attracting a custodial sentence of a maximum penalty of at least three years. Access and subscriber data could additionally be requested also by prosecutors, and for all categories of crime. European Preservation Orders could be issued by prosecutors, judges and courts, for all types of crime, and regardless of the type of data concerned.

- The proposal intends to 'move beyond' the model of direct cooperation between judicial authorities currently adopted by existing EU instruments of mutual recognition in criminal matters. Under the proposed regulation, the authorities of the member state where the measure is addressed would not be systematically involved in the execution of other member states' orders.

- It is proposed that the 'competent authorities' of the member state where an EPOC or EPOC-PR is addressed shall be consulted if the issuing state has reasons to believe that data requested is protected by immunities and privileges under the law of the country of execution, or that the disclosure may impact fundamental interests of that member state. Such duty to seek clarification is limited to production orders targeting content or transactional data.

- The intervention of judicial authorities in the member state where an EPOC or EPOC-PR order has to be executed might be required to enforce the investigative measure in the event that the private company concerned objects. The authorities of the member state of execution will have to enforce EPOCs or of EPOC-PRs that are not directly executed by the addressee of the order, unless they find that: non-compliance grounds as raised and identified by the addressed company are well founded; the data concerned is protected by an immunity or privilege under its national law, or; c) its disclosure may impact fundamental interests such as national security and defence.

- The Council of the European Union adopted its general approach on the draft regulation on European Production and Preservation Orders, proposing the establishment of a limited notification system. Notifications should only be given by the issuing authorities in specific circumstances, and only for orders targeting content data. The Council's general approach also proposes eliminating the possibility for addressees of an order to raise objections if it was apparent that the Order manifestly violets the Charter or it was manifestly abusive and foresees the introduction of new sanctions in case of non-compliance.

The European Commission proposed the introduction of a new set of rules on electronic information gathering for the purpose of, detecting, investigating, and prosecuting crime. These rules envisage conferring extraterritorial jurisdiction on member states' prosecuting and investigating authorities enabling them to address a private entity in another EU country directly, without the systematic *ex ante* involvement of the authorities of the member state in which the undertaking or its legal representative is located.

At the EU level, discussions on the need to create a tool facilitating access to electronic data for cross-border criminal proceedings took on particular salience in 2015 when the Commission presented the European Agenda on Security.[51] In April 2018, the Commission tabled two legislative proposals on the gathering of electronic evidence in criminal matters.

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 investigating and prosecuting authorities could issue to obtain a piece of electronic information directly from a service provider, as defined in Art 2 of the Regulation, if such provider is established in another member state or offers its services in the EU. 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 has been designed in view of allowing the member state issuing the Preservation Order to consequently secure production of the data sought (through a production order, or another available instruments), but it could originate from another member state conducting a criminal investigation or a third country, provided that the they are made aware of the preservation.

The second consists of a proposal for a directive that would introduce an obligation for 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

[51] 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.

EU to appoint at least one legal representative to act as a point of contact for Production and Preservation Orders addressed by the issuing authority. The proposal covers service providers wherever their headquarters are located or the information sought is stored, as long as they offer their services in the Union and they are not providing their services only on the own territory of the issuing member state. The company or its legal representative would be responsible - on behalf of the company - for "receiving, complying with and enforcing" orders and decisions issued by member states authorities competent for the purposes of gathering evidence in criminal proceedings, including the European Production and Preservation Orders proposed under the new e-evidence regulation.

In terms of material scope, the Commission's proposed regulation encompasses different categories of electronic information, covering both 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). The proposed regulation distinguishes between content data and transactional data on the one hand, and access data and subscriber information on the other.[52]

The proposal foresees that different authorities would be responsible for issuing the orders depending on the type of data sought.[53] Prior validation of a court would only be required for production orders concerning two categories of data (content and transactional) considered as having high "level of interference" with fundamental rights. These data could be requested for offences capable of resulting in a maximum custodial sentence of at least three years. Access and subscriber data could instead be requested not only by a judge and court, but also by a prosecutor, and for all categories of crime. European Preservation Orders (only ensuring preservation and not access to data) could be issued by a prosecutor, judge or court, for all types of crime, and regardless of the type of data concerned.

The new system envisaged to obtain electronic data would still rely on the authorities in the member state responsible for issuing an EPOC and/or EPOC-PR to assess the legality and proportionality of an order. The authorities of the EU country where the addressee is located would, instead, not be automatically involved in the process. The proposed regulation foresees that before the issuing of a production order some form of consultation might be required between the issuing state and the member state where the service provider is addressed, but only if the issuing authority has reasons to believe that the data requested are protected by immunities and privileges granted under the law of the country of execution, or that the disclosure may impact the fundamental interests of that member state.[54] Such a duty to seek clarification is furthermore limited to production orders targeting content or transactional data.

[52] Article 2(7)-(10) of the proposed regulation.

[53] Article 5 of the proposed regulation.

[54] Art. 5(7) of the proposed regulation.

Outside such circumstances, the intervention of the judicial authorities in the country of execution is only envisaged if the addressee of an order (the service provider or its legal representative) decides - based on its own assessment - to object its execution based on a set of limited non-execution ("non-compliance") grounds pre-identified in the proposed regulation (Stefan and González Fuster 2018, pp. 39-44).

According to the Commission proposal, the role of the judicial authorities in the member state where the addressee of an Order is located and has to be executed is therefore only incidental, and mainly directed at enforcing the investigative measure in the event where the private company concerned objects. The enforcement of EPOCs or of an EPOC-PRs that are not directly executed by the addressee is in fact required upon the authorities of the country of enforcement, unless they find that: a) non-compliance grounds - as raised and identified by the addressed company are well founded; b) the data concerned is protected by an immunity or privilege under the national law of the enforcing state, or; c) its disclosure may impact fundamental interests such as national security and defence.[55]

On 7 December 2018, the Council of the European Union adopted its general approach on the Draft Regulation on European Production and Preservation Orders.[56] The major amendment proposed by the Council in comparison to the text elaborated by the Commission is the establishment of a limited notification system. The Council's general approach foresees that notifications should only be given by the issuing authorities in specific circumstances, and only for orders targeting content data[57] which are considered *a priori* more sensitive.

When the issuing authority has reasonable grounds to believe the person whose data are sought is not residing on its own territory, the issuing authority must inform the enforcing state and give it an opportunity to flag whether the data requested may fall under the following categories: data protected by immunities and privileges; data subject to rules on determination and limitation of criminal liability related to freedom of expression/the press; and data whose disclosure may impact the fundamental interests of the state.

The issuing authority shall take these circumstances into account as if provided for under its own national law,[58] and it shall withdraw or adapt the order where necessary to give effect to these grounds. Such notification procedure was requested from several parties (Wahl, 2019). As far as the companies are concerned, the possibility of non-complying with an Order when it appears that its execution would result into a manifest violation of the EU Charter considerations has been

[55] Art. 14 of the proposed regulation.

[56] Council of the European Union, Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters - general approach, 15020/18, Brussels, 30 November 2018.

[57] Ibid., art 7a.

[58] Ibid. recital (35c)

eliminated from the Council's general approach. Furthermore, the proposal was made in the general approach of the Council to add a punitive sanction of 2% of turnover in case of non-compliance.

The Commission's proposals, as well as the general approach of the Council on the draft Regulation proved highly controversial among several groups of key stakeholders, as confirmed by the critical opinions expressed by EU bodies,[59] associations of legal professional,[60] industry organisatons,[61] as well as civil society representatives.[62] An extensive set of working documents produced by the European Parliament LIBE Secretariat and presented by the rapporteur and the co-rapporteurs during LIBE meetings also highlighted outstanding issues and raised doubts with regard to the legality, necessity and overall added value of the proposed instruments.[63]

[59] European Data Protection Board (EDPB), Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), adopted on 26 September 2018.

[60] ECBA Opinion on European Commission Proposals for: (1) A Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence & (2) a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

[61] EuroISPA's considerations on Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, June 2018.

[62] Civil society urges Member States to seriously reconsider its draft position on law enforcement access to data or "e-evidence".

[63] European Parliament, Public Register of Documents.

7. Cross-cutting challenges

KEY FINDINGS

- Under EU instruments of mutual recognition in criminal matters, judicial authorities of different member states are reciprocally required to trust that their decisions comply with the principles and values set forth in Article 2 TEU. The decision to allocate trust upon the member states authorities representing the judicial power ('judiciary') depends on the fact that only independent judicial authorities possess the statutory requirements and institutional capacity needed to duly perform the duty to protect fundamental rights in the context of criminal proceedings.
- In criminal matters, so far Article 82(1) TFEU has been used as legal basis for instruments of mutual recognition of decisions issued and executed by competent member states' judicial authorities. The duty to verify compliance with fundamental rights and the rule of law standards rely, in the first place, upon the authorities of the issuing member state, which have the responsibility of assessing the legality, necessity and proportionality of a cross-border measure entailing access to data sought for criminal justice-related purposes. On the other hand, the systematic ex-ante involvement of competent judicial authority in the country of execution remains crucial to verify the existence of the exceptional circumstances in the presence of which the principle of mutual recognition ceases to operate.
- Independent judicial scrutiny in the context of mutual recognition in criminal matters emerges as crucial for the operation of different instruments of mutual recognition, including those allowing to access, collect, and exchange data for the purpose of investigating and prosecuting and investigating crime. These constitute practices which affect fundamental rights and consequently call for effective judicial protection of potentially affected individuals under EU law. While implementing the EIO Directive, some EU member states still grant or envisage (either formally or in administrative practices) the power to issue data-gathering measure to police services.
- In the Commission's proposal for a Regulation establishing European Production or Preservation Orders, the issuing authorities would still be responsible for carrying out the assessment on legality, necessity and proportionality. Differently from existing EU law instruments for mutual recognition of judicial decisions in criminal matters, the proposed regulation would however do without the systematic *ex ante* involvement of competent authorities in the EU country where an order is to be executed. And yet, recent CJEU case law shows that judicial oversight in both the issuing and executing state remains central to maintain trust in the EU criminal justice area.
- The main qualitative difference between the EIO and the proposed Orders does not lie in differences between the authorities responsible for issuing or validating an order, but rather on the fact that the under the proposed Regulation there would not be a systematic involvement of the competent judicial authorities of the country of execution/enforcement which could secure effective remedies in cases where there is a lack of judicial independence, and risks of 'prosecutorial biases' exist in issuing countries.

- Fundamental rights concerns emerge from the analysis of the proposed e-evidence regulation. First, the proposed regulation would fail to systematically ensure effective judicial protection in cases where the issuing authority does not qualify as an independent judicial actor. Second, the assumption that production of preservation of some categories of data (subscriber and access) are a priori less sensitive from a fundamental rights perspective appears in tension with the CJEU jurisprudence and the constitutional traditions of several member states. Third, 'non-disclosure orders' might be issued without the need for the issuing authority to explicitly justify the necessity to keep the investigative measure secret. Such orders might potentially be issued in all criminal proceedings and would not necessarily be restricted to cases where notification to the data subject would put life, limb or property into danger. Fourth, complaint mechanisms and/or appeal procedures are limited in scope and only foreseen for Production Orders.
- Legal and practical challenges emerge from the perspective of the private sector. Companies noted that the limited information available in the certificate would render difficult to assess the existence of non-compliance grounds (as foreseen in the Commission proposal) and object the execution of an order. Service providers also expressed concerns about difficulties that would derive from the obligation to execute orders under significant time pressure, as well as with regard to the capacity to deal with potentially high numbers of requests. Furthermore, concerns have been expressed about the possible difficulties related to the seeking of reimbursement of costs before the authority of the issuing member state, instead of those of the country of execution.

7.1 Criminal justice challenges

Who issues and executes data requests for criminal justice purposes within the EU?

Mutual recognition of national judicial decisions in criminal matters has so far been only applied between judicial authority-to-judicial authority. Under existing EU instruments of mutual recognition in criminal matters, the judicial authorities in the issuing Member State are supposed to verify the legality, necessity and proportionality of a cross-border decision (Heard and Mansell, 2011). A residual but still crucial role is at the same time entrusted to the judicial authorities of the EU country where a cross-border criminal justice measure is to be executed. The *ex-ante* involvement of the competent judicial authorities in the member state of execution is needed to execute the measure on their territory. The executing authorities also have a central role for avoiding the recognition of an issuing member state's decision being translated into a violation of the rule of law or fundamental rights safeguards regarded as essential under the EU legal system and/or the national law of the executing country.

The judicial authorities competent for, respectively, validating and executing a criminal justice measure vary in each member state. Sometimes these authorities might be both judges and

prosecutors, depending on various factors including for instance the crime involved, the stage of proceedings, and the legal instrument used as legal basis.

Article 2 of the EIO Directive provides general definitions of who qualifies as issuing, validating and executing authority. Such authorities might vary according to the investigative measure requested, and the case concerned. The issuing authority might be a judge, a court, an investigating judge or a public prosecutor.[64] When in accordance with national law of the issuing country the gathering of evidence is ordered by an authority different from a court, judge or prosecutor, the EIO shall be validated by one of these judicial authorities, which remain responsible for examining the Order's conformity with the conditions for issuing an EIO.[65] As noted by Eurojust and the European Judicial Network (EJN) in their Joint Note on the practical application of the EIO, the EIO Directive has 'judicialised' the issuing phase by requiring EIOs to 'be issued by a judge, a court, an investigating judge or a public prosecutor competent in the case concerned (judicial authority as issuing authority), or by requiring that an EIO be validated by one of these authorities (judicial authority as validating authority).'[66]

As far as the recognition and execution of an EIO is concerned, Article 2(d) EIO DIR generally defines the executing authority as the 'authority having the competence to recognise an EIO and ensure its execution', as identified by the national law of the executing member state. While recognition and execution of an EIO is due to comply with formalities and procedures expressly indicated by the issuing authority, some important checks must still be performed by the 'competent authorities' of the county of execution. The latter are in particular due to verify that the measures requested in the EIO are 'not contrary to fundamental principles of law of the executing State'. Executing authorities might also take active part in the EIO's execution process also by assessing the opportunity to have recourse to a less intrusive investigative measure that the one indicated in the EIO when this would allow to achieve the same investigative/evidentiary result.[67] Furthermore, executing authorities are also called to assess the existence of one of the (limited and exhaustive) grounds of non-recognition provided under Article 11 of the Directive. As already mentioned, these grounds - which must be interpreted restrictively - also include the refusal to execute an EIO upon the identification of substantial grounds to believe that the execution of the investigative measure included therein would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter.

The possibility for the executing authorities to take into account their own national law when giving effect to EIOs, and their responsibility to examine the fundamental rights impact of received EIOs

[64] Art. 2 (c) (i) of the EIO Directive.

[65] Art. 2 (c) (ii) of the EIO Directive.

[66] Eurojust and European Judicial Network, 'Joint Note of Eurojust and the European Judicial Network on the practical application of the European Investigation Order', June 2019.

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

on the affected individuals call into question the possibility to perform such functions without the involvement of a competent judicial authority in the country of execution.

Restricting the operationalization of mutual recognition to cooperation among judicial authorities is justified considering that both the principle of separation of powers and the judicialisation of EU criminal justice cooperation constitute crucial conditions to maintain trust within the criminal justice area. That notwithstanding, some EU member states investigated by the JUD-IT Project still formally envisage or grant in administrative practices the power to adopt or execute fundamental right sensitive measures such as the access to and the collection of data sought in criminal proceedings to police services. In some cases, decision-making powers are even shifted in actual practice from the judiciary to law enforcement agencies. Human rights monitoring bodies such as the United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while countering Terrorism, and the Council of Europe Human Rights Commissioner have raised concerns about the case of France, in particular regarding the negative rule of law implications of anti-terrorism legislation and 'state of emergency'. In particular, these bodies deplored the blurring in the separation of powers in the country, indicating how such policy and legislative process prevents the exercise of *ex ante* effective judicial scrutiny over law enforcement measures, and undermines the constitutionally entrenched distinction between judicial and administrative police in the country.

The decision to allocate trust upon the member states judicial authorities depends precisely on the principle of separation of powers, and the fact that only the authorities representing the judicial power ('judiciary') possess the statutory requirements and institutional capacity needed to adequately perform the duty to protect fundamental rights in the context of criminal proceedings. Member states' judicial authorities are in fact those upon which the duty to protect and enforce rights arising from EU law primarily rely.[68] As Lenaerts stated, *"the authors of the Treaties took the view that national courts were best placed to protect the fundamental rights of individuals as they are insulated from political [private or commercial] considerations and are, in cooperation with the ECJ, entrusted with the task of upholding the rule of law within the EU"* (Lenaerts, 2017, p. 809). Two key questions that have been posed to the CJEU along the years are thus: who qualifies as a 'judicial authority', and who is an 'Issuing Judicial Authority' possessing the level of independence from the executive required to maintain the high level of mutual trust required for the functioning of EU criminal justice cooperation?

Member states' police services have been considered as 'non-judicial authorities' by the CJEU in Case C-452/16 PPU, *Poltorak*. Here the Luxembourg Court concluded that the issuing of an EAW by a police service *"does not provide the executing judicial authority with the assurance that the issue of that EAW has undergone such judicial approval and cannot therefore suffice to justify the high level of [trust] between the Member States".* Such an exclusion is justified in light of the need

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

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 criminal justice cooperation on the other. At the same time, the Court stressed that the concept of 'judicial authority' does not coincide with the narrower one of *'independent judicial authority*'. According to the CJEU, this latter category only includes public bodies which, while participating in the administration of criminal justice, act independently from the executive. As a consequence, the notion of 'independent judicial authority' cannot encompass authorities, such as ministries or police, which are "within the province of the executive".[69] This is of central importance in order to ensure the correct implementation by EU member states of the EIO Directive.

In the much debated Case C-216/18 *PPU LM,* the CJEU in particular highlighted the importance to secure judicial independence within the context of mutual recognition proceedings - and the EAW more specifically - by stressing 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 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.[70] With this judgment, the Court reaffirmed the centrality of the independent judicial oversight by 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.

On the one hand, the Court confirmed that judicial authorities in the executing country have an independent responsibility to put a halt to a mutual recognition request if – based on the results of the 'two-step test' developed in occasion of the *Aranyosi and Căldăraru*[71] case – it results that its execution would generate a real risk of violation of the concerned individual's fundamental right to a fair trial before an independent tribunal. On the other hand, the CJEU established in the *PPU LM* case that the high level of judicial independence required to secure the effective judicial protection afforded under EU law should already be ensured at the moment when a cross-border decision – and most notably an EAW – adopted in the context of EU mutual recognition proceeding is issued. The Court referred to its decision on the *Associação Sindical dos Juízes Portugueses* case,[72] in order to emphasise the key importance of judicial independence and impartiality for fair trial rights to be respected.

[69] 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, para 35.

[70] 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.

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

[72] Case C-64/16.

In May 2019, the CJEU dealt with the extent to which German public prosecutor offices could be considered as 'judicial authority' for the purpose of the EAW.[73] The case originated from preliminary reference requests from the Irish Supreme Court, which considered the execution of three EAWs issued prior to judgment for the purposes of conducting a criminal prosecution respectively by two German public prosecutor offices (Lübeck and Zwickau). The referring Irish court asked the CJEU for guidance about the EU law concept of "issuing judicial authority" for the purposes of issuing an EAW. The CJEU held that the issuing authority in an EAW case "must be in a position to give assurances to the executing judicial authority that it acts independently in the execution of those of its responsibilities". It added that "*That independence requires that there are statutory rules and an institutional framework capable of guaranteeing that the issuing judicial authority is not exposed, when adopting a decision to issue such an arrest warrant, to any risk of being subject, inter alia, to an instruction in a specific case from the executive.*"[74]

The Court added that a clear sign of a lack of independence was the power of the Ministry of Justice to exert 'external power' to issue instructions to public prosecutor offices, and directly influence the latter in issuing or not a decision. The CJEU highlighted that any existing safeguards related to the power to issue instructions could be changed in the future "by political decisions" and that the existence of any possibility to be exposed to the risk of being subject – directly or indirectly – to "directions or instructions" from the executive would suffice to conclude the non-independence of the prosecutorial authority.[75] It therefore concluded that German prosecutorial authorities cannot be considered as 'issuing judicial authorities' for the purposes of the EAW. The Court has in this way provided a uniform and autonomous interpretation of these notions or concepts for the purposes of EU law.

The Court thus made it clear that ensuring effective judicial protection in the context of EAW proceedings requires the systematic involvement of independent judicial authorities. Not only does the Court confirm that the independence of judicial authorities is essential to guarantee effective judicial protection of individuals, but expressly requires several EU countries to either: align their public prosecution services with the judicial independence benchmarks mentioned above, or; subject their decisions to the independent judicial oversight mechanisms required to secure judicial protection of fundamental rights in mutual recognition cases.[76]

In *PPU OG and PI*, the Court explicitly interpreted the concept of 'judicial authority' within the meaning of the EAW Framework Decision, and taking into account in particular the wording of Article 6(1) of that piece of EU legislation. Furthermore, in the case at hand the CJEU explicitly refers to the right to liberty.

[73] Joined Cases C-508/18 and C-82/19 *PPU OG and PI* of 27 May 2019.

[74] Ibid., Paragraph 74.

[75] Ibid. Paragraphs 83 and 86.

[76] https://www.fairtrials.org/sites/default/files/publication_pdf/CJEU_27_May_2019_cases_IP_LB_final.pdf

At the same time, in a context where there is no guarantee that cross-border investigative measures are subject to effective judicial oversight in the country of issuance or execution, the question arises as to how to ensure the sufficient level of judicial protection required by EU law to adequately safeguard other fundamental rights, such as the right to privacy, which might be negatively impacted by the execution of an order mandating a private company to provide investigating or prosecuting actors access to personal data. The question applies to both EIOs (in cases where they are issued and executed by judicial authorities that are not independent, or in cases where they are only 'formally' issued, validated and/or executed by a judicial authority) and, to a different extent, to the Commission proposal on e-evidence.

As far as the EIO is concerned, it is worth remembering that several of the different authorities currently listed as 'competent for issuing EIOs'[77] are not recognised as judicial authorities across the EU. For instance, it was noted that Italy's criminal procedural law does not make it possible to consider UK barristers' associations as judicial authorities. In practice, an EIO written by a UK barristers' association might be considered a valid measure (and consequently executed) by Italian authorities, provided that it is signed by a UK court. And yet, securing effective scrutiny by an independent judicial scrutiny appears central in the context of EIO proceedings. This emerges, for instance, from the fact that member state courts are starting to interrogate the CJEU as to the type of the level of legal protection and type of remedies to be afforded in the country of issuing to persons other than the accused, who may also be subject to measures leading to the acquisition of electronic data[78] (Whal, 2019a).

Furthermore, while not requiring the systematic involvement of independent courts in all cases, the EIO still 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. Under the EIO 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.

According to the Court decision in *PPU OG and PI*, the EAW system "entails a dual level of protection of procedural rights and fundamental rights which must be enjoyed by the requested person, since in addition to the judicial protection provided at the first level, at which a national decision is adopted, there is the protection afforded at the second level, at which the EAW is issued" (paragraph 67). While the main responsibility for safeguarding fundamental rights in the

[77] European Judicial Network, Competent authorities, languages accepted, urgent matters and scope of the EIO Directive in the EU member states (https://www.ejnforum.eu/cp/registry-files/3339/Competent-authorities-languages-accepted-scope-EIO-181218.pdf).

[78] C-324/17 (Criminal proceedings against Ivan Gavanozov).

EAW lies with the dual system of protection in the issuing member state, the design of existing EU mutual recognition in criminal matters and the case law of the CJEU reconfirm that the oversight regime adopted by existing mutual recognition instruments depends on the involvement of judicial authorities in both the issuing and executing state.

The new e-evidence proposals would change this two-level system of protection to only one in the issuing EU member state (for EPO-PR and in cases where the EPO targets subscriber and access data); and potentially to none in the list of EU countries where prosecutors do not meet CJEU independence standards. Indeed, as Table 2 below shows, Germany is not the only EU member state among those covered by the JUD-IT project that cannot be considered as an 'issuing judicial authority' for the purposes of the EAW. Other clear cases include Austria, France, Luxembourg and the Netherlands.

Table 2. JUD-IT member states prosecutorial authorities

Country	Instructions in Individual Cases from Executive	General Guidelines on Policy from Executive	Management Powers by Ministry of Justice	CJEU 'Independence' Test
Austria	X	X	X	
Belgium		X		
Bulgaria				V
France		X	X	
Germany	X	X	X	
Greece				V
Hungary				V
Ireland				V
Italy				V
Luxembourg	X		X	
Spain				V
Sweden		X		
The Netherlands	X	X	X	

Source: EU Justice Scoreboard, 2018; and JUD-IT Country Reports.

As the Council of Europe's European Commission for Democracy through Law (better known as the Venice Commission) put it: "While the independence of judges and the judiciary in general have their origin in the fundamental right for persons to a fair trial [...] the independence of prosecutors

and the prosecution system does not have such a common standard."[79] "[...] [T]he major reference texts allow for systems where the prosecution service is not independent from the executive". "Nonetheless, where such systems are in place, guarantees must be provided at the level of the individual case to ensure that there is transparency concerning instructions that may be given."[80]

7.1.1 The involvement of judicial authorities in the issuing and executing country

There is a qualitative difference between the role currently entrusted to the state of execution under existing EU instruments of mutual recognition in criminal matters, and the one reserved to the 'enforcing state' under the Commission proposal for a regulation under the e-evidence package.

As already noted, the latter foresees that the executing state's authorities only possibly and incidentally participate in the execution phase. In such a context they do not take relevant criminal justice decisions with far-reaching implications for fundamental rights based on the direct assessment of the information provided by the issuing authorities (i.e. the information contained in the EPOC/EPOR-PR as well as the reasoning on necessity and proportionality), but only in the eventuality that a procedure for enforcement is initiated, and on the basis of the addressee's opposition to the order. This means that the decision whether or not to execute a cross-border data-gathering measure to obtain data would no longer follow a direct and systematic assessment by the competent executing authority of the grounds for non-recognition or non-execution of the issuing member state's evidence gathering measure. The involvement and scrutiny of another member state's Order would instead become dependent on the existence, content and quality of a prior objection raised by the company in light of the (scant) information made available in the order.

The proposed regulation thus foresees a shift from a system (that of the EIO) where the judicial control and fundamental rights scrutiny that is "redolent of a request for evidence" is conducted by competent public authorities in the executing member state (Mitsilegas, 2018) to one in which the involvement of the latter is mainly a function of the enforcing foreign authorities' criminal jurisdiction, and exercised in a way which is intermediated by the eventual hypothesis of opposition and non-compliance of the private company. Such move has been justified in light of considerations linked to the special (volatile) nature of electronic data and the different level of intrusiveness in fundamental rights that data-gathering measures adopted in the area of criminal justice have when compared to the EAW. It has furthermore been noted that in some cases the factor connecting a member state with the criminal proceeding would 'only' be the location of the data sought, or the fact that the company holding the data sough is established (or appointed its legal representative) there.

[79] (CDL-AD(2014)029, Opinion on the Draft amendments to the Law on the State Prosecutorial Council of Serbia, §7).

[80] (CDL-AD(2014)042, Interim Opinion on the Draft Law on the State Prosecution Office of Montenegro, § 16).

As consequence, in the Commission's proposed regulation verifying that all safeguards prescribed by EU law in the field of criminal justice and data protection will be *de jure* and *de facto* entrusted exclusively to the authorities of the issuing country. However, this appear to be a dangerous choice in a context where different EU countries are undertaking legislative reforms (including of the judiciaries), which effectively weaken basic rule of law and fundamental rights protections. The deterioration of judicial independence and the rule of law in several EU countries, is evidence that respect of fundamental rights and other basic legal protections cannot always be taken for granted within the EU (Bárd, 2018).

Substantial differences also existing between the limited notification' system envisaged in the Council's general approach on the draft Regulation and the type of judicial cooperation currently upholding already existing EU instruments of mutual recognition in criminal matters. In the first place, such notification system would not entail an automatic and systematic involvement of the judicial authorities of the country where an order is addressed, as it would be limited to specific cases and circumstances. The notification system provided by the general approach would neither give the competent oversight authorities of the member state where the order is addressed the possibility to raise fundamental rights concerns should they arise, and be different from the ones included in the proposed legislative text.[81] Also, since the notification to the member state of execution would not have suspensive effect, there would be no guarantees that the access or transfer of data would be stopped in cases where issues are flagged. The involvement of the state of execution under the proposed notification system is therefore not systematic, and does not grant the authorities of the member state where the addressee of an order for content data is located with the possibility to raise non-recognition/non-execution grounds.

Important divergences also emerge when comparing the notification system envisaged under the Council's general approach on the e-evidence regulation with the one established under Art. 31 of the EIO Directive, which applies to the interception of telecommunications of a subject located in the territory of a EU country different from the 'intercepting member state'.

Similarly to the notification mechanism foreseen in the Council's general approach, the one included in the EIO does not have a suspensive effect *stricto sensu*. However, according to Art. 31 the EIO Directive the intercepting member state shall always and systematically notify the competent authority of the other member state concerned by the interception. Notification shall occur prior to the interception whereas the competent authority of the intercepting member state already knows (at the time of ordering the interception) that the subject of the interception is or will be on the territory of the notified member state.[82] Lacking an *ex ante* notification, the intercepting member state shall comply with the notification duties during or immediately after

[81] The possibility for the service provider to oppose the execution of the Order on the basis of manifest violations of the Charter has also been removed in the Council General Approach on the proposal.

[82] Art. 32(1)(a).

the interception. Exception to the *ex-ante* notification requirement are furthermore only allowed if the intercepting member state only becomes aware that the subject of the interception is or has been on the territory of the notified Member State after ordering the interception.[83]

Another difference concerns the possible reactions of the competent authority of the notified member state. Under the EIO Directive, the latter is given the possibility to notify the intercepting member state that the interception may not be carried out or shall be terminated by the competent authority of the intercepting Member State. Where necessary, the notified member state might also notify the intercepting members state that any material already intercepted may not be used, or may only be used under conditions which it shall specify. In such case, the competent authority of the notified member state shall inform the competent authority of the intercepting member state of reasons justifying those conditions.

As such, the way of working of the proposed instrument, included as envisaged by Council general approach, still departs from the model of cooperation featuring current mutual recognition instruments, where decisions come from a judicial (or equivalent) authority in the issuing state and are directly 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.

7.1.2 Legal basis and the specificities of mutual recognition in EU criminal justice

The Commission choice of Article 82(1) TFEU as the legal basis for the proposed regulation on European Production and Preservation Orders for electronic evidence in criminal matters has been a point of controversy and disagreement.

Article 82 TFEU provides a legal basis for judicial cooperation based on mutual recognition. According to Art. 82(1)(a), the European Parliament and the Council shall adopt measures to lay down rules and procedures for ensuring recognition throughout the Union of all forms of judgments and judicial decisions. Only Art 82(1)(d) specifically refers to judicial cooperation between judicial or equivalent authorities. Art. 82 (1) (a) TFEU does not require the involvement of judicial authorities in two member states as an obligatory element of mutual recognition.

In some areas of EU law, the principle of mutual recognition is fully respected when a judicial decision of an authority in a member state has legal effects in another member state, without the prior intervention of another authority in that other member state. At the same time, while this form of mutual recognition has been already established in other areas of EU legislation, such as in civil matters, and in the internal market, it has never been applied to EU legislation in criminal matters. There is a fundamental difference between the mutual recognition principle in the context of criminal law, and other areas of European law such as civil and private law.

[83] Art. 32(1)(b).

While private and commercial law decisions can also have far-reaching implication on individuals' rights, measures adopted in the field of criminal law are based on a very specific relationship between the state and the individual. Criminal justice decisions systematically impinge on fundamental rights and freedoms of individuals, and they encroach upon punitive powers at the heart of member states' sovereignty. The latter have agreed over the years to give up some of their longstanding prerogatives to set up a system of unprecedented cooperation. Yet, this has been possible within a context where a number of safeguards are guaranteed. Oversight of judicial authorities of other member states decisions' compliance with fundamental rights standards set out in the EU Charter and in national constitutions appears as a crucial requirement in that respect.

When it comes to criminal justice cooperation there are not only very sensitive (sovereign) interests at stakes, but disputes in criminal cases also involve a relationship between two unequal parties. The prosecution has the 'machinery of the state behind it' and acts adopted in the context of criminal investigations and/or prosecution might have far-reaching consequence for the fundamental rights of suspects or accused persons.[84] Unlike in the other areas of EU law where the principle of mutual recognition applies, abuses of mutual trust and mutual recognition in the criminal justice area *'have different, considerably graver consequences for the individual.'* (Bárd, 2018). Bard observed how in the context of criminal justice cooperation, faulty judgments but also blind trust and automatic recognition of foreign measures will in all cases and necessarily result in individual rights' infringements, but also rule of law and human rights violations. As a consequence, she notes how in the criminal justice domain it is only allowed to *presume* the good intentions and adherence of member states to Article 2 TEU values, which makes the need to ensure adequate judicial scrutiny by the competent authorities of the member state of execution of cross-border decisions even more compelling.

In a letter adopted in reaction to the Commission e-evidence proposal, Members of the Council further stressed that 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.[85] In one of the first working documents adopted after the publication of the Commission's proposal, the authors (rapporteur Birgit Sippel, and shadow rapporteur Nuno Melo) from the European Parliament's LIBE Committee recalled the importance to interpret EU primary law provisions related to criminal justice strictly in order to avoid a "non-solicited and hidden Treaty change".[86] The authors of the working paper also noted that all past criminal justice mutual recognition

[84] Fair Trials (2019), Consultation paper on cross-border access to electronic data.

[85] Ministries of Justice of Germany, The Netherlands, Czech Republic, Finland, Latvia, Sweden, Hungary, Greece (2018), Letter to Mrs Věra Jourová, 20 November.

[86] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 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, 24 January 2019, p 3.

instruments that have 'explicitly been based on Article 82(1)(a), have been targeted at judicial authorities and prescribed the recognition of judgments and judicial decisions'.[87] Arguing that the 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 (EDPB) has also questioned the appropriateness of the Commission's choice of legal basis.[88]

In the EU legal system, the choice of the appropriate legal basis has a 'constitutional significance'. Having only conferred powers, the EU must strictly link the acts it adopts to the Treaty provisions that actually empower it to adopt such acts (Docksey, 2018). According to the Court of Luxembourg, an act of the Union is strictly linked to a Treaty provision when the "main aim or component" of the measure in question is in line with the one underpinning the selected legal basis.[89] Direct public-private cooperation for cross-border gathering and transfer of data differs substantially from the type of cooperation that article 82 TFEU prescribes for judicial cooperation in criminal matters.

The landmark CJEU (Grand Chamber) Opinion on the draft EU-Canada Passenger Name Records (PNR) Agreement[90] also provides guidelines that are useful for the selection of the appropriate legal basis of EU initiatives aimed at enabling the cross-border collection, storage, processing, analysis and exchange of information for the purpose of - inter alia - detecting and investigating crime. In its Opinion in case A-1/15 the Court analysed the aim and content of the envisaged PNR Canada agreement. In accordance with the consolidated case-law on the choice of the legal basis, CJEU recalled how the latter must be founded on objective criteria amenable to judicial review, and how those objective criteria include the purpose and the content of the act at issue.

With regard to the draft agreement at hand, the Court of Luxembourg withheld a double legal basis: protection of personal data (Art. 16 TFEU) and police cooperation in criminal matters concerning the exchange of information (Art 87(2)(a)). The CJEU found that the purpose of the agreement under scrutiny was in fact to combat terrorism and serious transnational crime "while safeguarding the right to respect for privacy and the right to protection of personal data". To reconcile the two objectives - both recognised by the Court as constituting two essential components of the Agreement - the legal basis was therefore to be found under the headings of police cooperation along with data protection, and not public security and the activities of the state in areas of criminal law (Carrera and Mitsilegas, 2017).

[87] Ibid. p. 5.

[88] 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.

[89] Case C-178/03 Commission of the European Communities v European Parliament and Council of the European Union, para. 1.

[90] 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.

The CJEU Opinion PNR Canada agreement also dealt with the question of whether Article 82(1) constituted the appropriate legal basis for a system of international cooperation between a private provider based in the EU and a law enforcement authority in a third country. Upon the consideration that none of the provisions of the envisaged agreement referred to facilitating judicial cooperation, the Court discarded Article 82 TFEU on judicial cooperation on criminal matters as possible legal basis. The CJEU stated in particular that Article 82(1)(d) can only provide the legal basis for measures facilitate cooperation between two judicial authorities, while cooperation between law enforcement and private providers is not covered.[91]

Being an initiative directed at enabling direct enforcement by private companies of cross-border measures issued by member states' investigating or prosecuting authorities, the proposed regulation appears to lack one of the essential elements that so far have characterised EU mutual recognition instruments of judicial cooperation in criminal matters, and most notably the direct and systematic contact between competent judicial authorities (including both judges and prosecutors) in the issuing and executing member state. As a consequence, it appears that purpose and the content of the proposal at issue fall outside the scope of the Treaty provision chosen for its legal basis by the Commission.

Expert consulted during the JUD-IT project have furthermore raised doubts as to the possibility for the EU to use Art. 82 of the TFEU to adopt initiatives that would *de facto* lead to the abandonment of member states sovereignty to execute the law in their respective territory. In fact, Article 89 of the TFEU indicates that the EU can adopt measures empowering member states' to operate in the territory other EU country only when cooperation occurs 'in liaison and in agreement with the authorities' of the latter.

In relation to the protection of personal data, the Commission's proposal does explicitly refer to the need to respect the fundamental right to the protection of personal data 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.

7.2 Conflicts of laws

A specific set of challenges emerge in relation to data requests issued by EU countries' investigating and prosecuting authorities and addressed directly to service providers in the US. Companies

[91] Para. 102.

falling under US jurisdiction can provide non-content data to foreign authorities, but pursuant to Section 2701(2) of the Electronic Communications and Privacy Act 1986 (ECPA) they are prohibited from sharing content data with foreign law enforcement authorities. The SCA, which is contained in Title II of the ECPA, acts in fact as a blocking statute that limits the possibility for foreign governments to directly request content data held by IT companies in the US. It does so by subjecting their possibility of accessing electronic information to the requirement of *ex ante* independent judicial validation by a US court. The content of electronic communications might only be produced when a US federal judge has been satisfied of the existence of 'probable cause'.[92] On the other hand, even when an order meets the probable cause standard, service providers in the US are not allowed to respond to direct orders (or: 'requests') from EU authorities. Some exceptions to such rules have been introduced in practice in relation to 'emergency requests'. The US law allows US service providers to respond to these requests following the policies and standards set out by the service providers themselves and irrespective of the 'probable cause' standards being met.[93]

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 in force in the (non-EU) foreign legal system where they are established (e.g. the US). Therefore, under the proposed regulation the risks of a conflict of laws are still likely to arise when European Production or Preservation Orders are issued for content data falling under US jurisdiction. As already noted, the Fourth Amendment requires a US judicial authority to issue a warrant with probable cause to provide foreign authorities access to the content of electronic communications. It is far from certain that in the absence of such a warrant, US service providers will be able to provide EU member state authorities access to the requested data without incurring liabilities under US law.

[92] 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. 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.

[93] European Commission (2018), "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, p. 84-85.

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" of the service provider, the issuing authority may choose whether to withdraw the order or to uphold it.[94] 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 if the law of the third country applies to the case, if a conflict of law actually exists, and to assess the lawfulness of the foreign legislation protecting the data against access.

In carrying out the assessment, the issuing member state's 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 law enforcement requests for 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. 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.

7.3 Constitutional and fundamental rights challenges

7.3.1 Constitutional identities in the EU and the essence of constitutional rights

The extent to which national constitutional specificities and different legal traditions provide limits to criminal justice cooperation between member states has long constituted a matter of debate among EU and member states' judicial authorities, as well as between legal scholars.

The relationship between EU law and national constitutional law in the context of the operation of the principle of mutual recognition in criminal matters has been examined in the case of *Melloni*.[95] In such case, the Court decided that the higher level of fundamental rights protection ensured by national constitutional law cannot compromise the primacy of EU secondary law (the European Arrest Warrant Framework Decision as amended by the Framework decision in judgements in absentia, interpreted in light of the Charter).

By establishing that member state are, in principle, obliged to act upon a EAW, the CJEU has a adopted a 'teleological interpretation' (Mitsilegas, 2015) of the relevant legal basis for such mutual recognition instrument, and backed a literal understanding of Art. 4a(1) of the EAW Framework

[94] See in particular Articles 15(1), 16(1) and 2(1) of the proposed regulation.

[95] Case C-399/11, *Melloni*, Judgement of 26 February 2013.

Decision by finding that this provisions restricts the opportunities for refusing to execute an EAW.[96] The *Melloni* judgement has thus in principle deprived national executing authorities of any discretion to examine the compatibility of the execution of a EAW with fundamental rights in a wide range of cases involving in absentia rulings. By giving priority to the effectiveness of mutual recognition based on presumed mutual over national constitutional law which provides a high protection of fundamental rights, the Court has interpreted fundamental rights in a restrictive manner. And yet, the focus put by the Court on the importance to operationalize a system of quasi-automatic mutual recognition can raise serious challenges from the perspective of effective fundamental rights protection.

According to Lenaerts, "the executing authority may not make the execution of an EAW conditional upon compliance with the level of fundamental rights protection provided by its own constitution where that level is higher than that provided by EU law…. [imposing] its own constitutional standards…would be the beginning of the end of principle of mutual trust". However, he has also underlined however that "mutual recognition of judgments should not operate to the detriment of fundamental rights" (Lenaerts, 2017, pp. 814 and 823).

Bárd and van Ballegooij noted that the tendency of the CJEU to limit the discretion of executing judicial authorities not only misinterprets the principle of mutual recognition, but also negates the concept that fundamental rights are a direct source of EU law in the EU Charter of Fundamental Rights (Bárd, and van Ballegooij, 2019). Moreover, van Ballegooij (2015) has argued that "Limiting the discretion of executing judicial authorities, claiming that it is good for mutual recognition fails to understand the need to recognise judicial decisions as opposed to enforcing them directly based on compliance with the standards of the home state (home state control)".

The CJEU seems to have later accepted such arguments, as confirmed by the conclusions of judgements such as *Aranyosi and Caldararu,* in the context of which the Court recognised *that* that the principle of mutual trust "may be limited where the execution of an EAW is liable to give rise to breaches of the prohibition of torture and inhuman and degrading treatment enshrined in Article 4 EU Charter". In its ruling *Minister for Justice and Equality v LM* of 25 July 2018,[97] the Court extended the two-step *Aranyosi* test to cases where the rule of law is at stake, and the right to an effective remedy and fair trials envisaged in Art. 47 of the EU Charter.

The 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). Recent normative developments in the EU criminal justice field show that the execution of a 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

[96] Para 41.

[97] Case C-216/18 PPU Minister for Justice and Equality v LM (Deficiencies in the system of justice), Judgment of 25 July 2018.

comply.[98] Such a nucleus includes the primary fundamental rights and rule of law standards that are provided for by both the EU and/or the executing Member State's constitutional and legal systems (Lenaerts, 2015).

The EIO model has also enshrined these national diversities by including as express ground for non-execution which can be raised by the executing authority upon the finding that complying with the formalities and procedures expressly indicated by the issuing authority would be contrary to the fundamental principles of law of the executing state.[99] Some of these may relate - directly or indirectly - to fundamental rights, but some other equally important elements may correspond with other key legal criteria such as national security interests.[100]

National constitutional courts have already signaled the limits of the primacy of EU law and the mutual recognition principle, and the limits of 'blind' automatic operability of mutual recognition in criminal justice matters. The relationship between EU law and constitutional and criminal justice traditions remains an evolving and contested one. Some national constitutional courts have remained rather consistent regarding 'uncritical trust' in cases of mutual recognition of judicial decisions in criminal matters, as the follow up of the CJEU *Melloni* case clearly demonstrates.

Germany constitutes a case in point, as exemplified by the German Constitutional Court's decision of 15 December 2015.[101] Such decision concerns an identity check for a person subject to a EAW based on a verdict in absentia and the rights of the arrested person to challenge such decision. The BVerfG held that mutual trust has limits and that it can be challenged "if there are indications based on facts that the requirements indispensable for the protection of human dignity would not be complied with in the case of an extradition". The requirement to carry out a "constitutional identity review" by the Constitutional Court - which may lead to situations where EU criminal law may be inapplicable - remains, to date, unresolved. Mitsilegas concluded that the German Constitutional Court 'introduced the requirement of identity review of measures implementing the EAW when the principle of human dignity is at stake' (Mitsilegas, 2019, p. 425).

The existence of the state's responsibility to protect its citizens' fundamental rights in line with national constitutional requirements has been considered by German Constitutional Court also with regard to international cooperation measures directed at enabling cross-border access to

[98] Before the entry into force of the Lisbon Treaty, EU mutual recognition instruments contained references to the respect of fundamental rights but did not include a specific ground for refusal in this regard. Post-Lisbon Mutual recognition instruments foresee grounds for refusal based on a fundamental rights assessment in the country of execution. See for instance, Art. 8(1(f) and Art. 19(1)(h) Regulation (EU) 2018/1805/EU of the European Parliament and of the Council on the mutual recognition of freezing orders and confiscation orders. The Regulation foresees a ground for non-recognition based on fundamental rights, although its exercise is only possible under very strict conditions.

[99] Art. 9(2) of the EIO Directive.

[100] Art. 11(1)(b) of the EO Directive.

[101] BVerfG Order, 15 December 2015 (2 BvR 2735/14).

personal data.[102] In in its ruling on Art. 32 of the Council of Europe Convention on Cybercrime, as ratified by the German legislature, the German Constitutional Court considered the existence of the state's responsibility to protect its citizens against fundamental rights violations resulting from cross-border access to personal data. In the case at hand, the BVerfG dismissed the complaint because of the applicant's failure to substantiate the alleged fundamental rights violation.

And yet, an opposite conclusion was reached by a dissenting opinion arguing that the Cybercrime Convention's provision under scrutiny violated the applicant's privacy rights, most notably by authorising foreign authorities to access personal data without providing effective protection against violations of privacy rights resulting from such access.[103] In his assessment of the Commission's proposal on electronic evidence, Böse reported how the Upper House of the German Parliament representing the states (Bundesrat) referred to the Constitutional Court's ruling to raise similar objections with regard to the envisaged Regulation (Böse, 2018).

In Spain, the Constitutional Tribunal response to the CJEU *Melloni* judgment represents another illustrative example that the automaticity of mutual recognition in EU criminal law remains constitutionally unsettled and unresolved. The Spanish Constitutional Court found a key conundrum: the CJEU ruling in *Melloni* versus its own case law covering suspects rights in the scope of trials *in absentia*. As Bachmaier Winter has rightly pointed out, instead of creating a direct clash with Luxembourg, the Spanish Court "compromised and made an intelligent move, which consisted in presenting those contradicting positions as compatible" (Bachmaier Winter, 2019, p. 408).

The Spanish Constitutional Court agreed to revise its own jurisprudence on trials *in absentia* while not expressly acknowledging that this resulted from the supremacy of EU criminal law in the Spanish constitutional system. It held that the Spanish Constitution's recognition of the primacy of EU law (Art. 93 Spanish Constitution) is dependent upon limits emerging from "the respect for the sovereignty of the state, our basic constitutional structures and value system and fundamental principles, where the fundamental rights hold their own substantive nature" (Art. 10 Spanish Constitution).[104] Centrally, the Spanish Constitutional Court concluded that in the occurrence of "the unlikely situation" where EU law would end up incompatible with the Spanish Constitution, the preservation of the sovereignty of the Spanish people and the supremacy of the Constitution could in the last instance lead the Court to tackle such problems.[105]

Sweden is another case in point, where principles of freedom of the press and freedom of expression find particular constitutional protections in its national legal system (SE). This

[102] Bundesverfassungsgericht [German Federal Constitutional Court], Decision of 21 June 2016, 2 BvR 637/09, official court reports [BVerfGE], Vol. 142, p. 234, 249 and following.

[103] Dissenting opinion of Judge Huber, ibidem, at 257 and following.

[104] Declaration 1/2004 (DCC).

[105] DTC 1/2004, 13 December, FJ 4.

sometimes constitutes a barrier to mutual recognition-based instruments as their domestic courts will not accept items of evidence in cases where the legal representative has not been informed.

7.3.2 Privacy

The proposed E-evidence regulation distinguishes between content data and transactional data on the one hand, and access data and subscriber information on the other.[106] The proposal foresees in particular that different authorities would be responsible for issuing the orders depending on the type of data sought.[107] Prior involvement of a judge or court would only be required for production orders concerning two categories of data (content and transactional) which are considered as having a high "level of interference" with fundamental rights. These data could be requested for offences capable of resulting in a custodial sentence of at least three years. Access and subscriber data could instead be requested for all categories of crime and directly by prosecutors, without necessary requiring the intervention of a court or judge.

The idea according to which subscriber and access data systematically deserve a lower level of protection appears has been considered in tension with the EU data protection law and the basic standards that the latter generally applies to all personal data. Article 8 of the EU Charter applies to any processing of personal data. Although it is true that some special types of personal data are characterised as 'sensitive' and consequently granted additional protection, and that certain types of processing are regarded as involving a higher risk and thus subject to more stringent rules, this should not be interpreted as allowing gradations depriving certain categories of information of basic data protection standards.

According to the Explanatory Memorandum accompanying the proposal, personal data covered by the envisaged regulation are 'protected and may only be processed in accordance with the EU data protection *acquis*, ad most notably with the General Data Protection Regulation (GDPR) and the Data Protection Directive for Police and Criminal Justice Authorities (Law Enforcement Data Protection Directive)'.[108] The proposal also recalls that the regulation cannot alter fundamental rights obligations derived from Article 6 TEU. At the same time, the proposal does not provide a clear justification for the lowering of substantial and procedural safeguards that is envisaged for subscriber and access data.

The proposal seems to base the decision to grant a lower level of safeguards to subscriber and access data upon the assumption that access to such information only entail limited levels of interference with fundamental rights. It does however not provide detailed explanations as to how different such interference would be for subscriber and access data. Furthermore, it is not clear why the levels of interference would be coincidental for these two categories, and for instance in

[106] Article 2(7)-(10) of the proposed regulation.

[107] Article 5 of the proposed regulation.

[108] Recital 20 of the proposed regulation.

which way the level of interference with fundamental rights of access data can always be considered 'similar to that of subscriber data'.[109]

The presumption according to which requests of and access to these categories of non-content data (can be a priori and in all cases considered less intrusive from a fundamental rights perspective is also contradicted by the fact that, in several EU countries covered by the JUD-IT project, a court authorisation is necessary for these specific type of electronic information.[110]

Furthermore, making a clear-cut distinction between specific categories of data is not always an easy task. This is particularly the case when it comes to dynamic IP addresses. In fact, dynamic IP addresses are assigned to specific users each time they log into the account(s) they have on specific devices and/or networks. Consequently, in order to identify the user to which a dynamic IP address was assigned to a specific point in time, investigating and prosecuting authorities need to collect transactional and access data. Without the latter it would in fact not be possible to determine the identity of the persons behind the IP address. Depending on the specific circumstances of a case at hand, this type of data might therefore require higher level of protection that the one currently foreseen in the draft regulation. Under the proposed regulation the risk exists that the issuing authority qualify these type of dynamic IP addresses as subscriber information, while instead they constitute traffic data revealing circumstances and facts connected to the electronic communication. In such cases, these data would require a higher level of protection that the one currently foreseen in the draft regulation for subscriber or access data[111]

The CJEU has ruled that when metadata (such as traffic data and location data) provides the means of establishing a profile of the individuals concerned that such information is no less sensitive, having regard to the right to privacy, than the actual content of communications.[112] The ECtHR has also 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.[113] These issues must be considered in addition to the fundamental requirement of conditioning the acquisition by a public authority of

[109] Recital 21 of the proposed regulation.

[110] See Cyber Crime Committee, T-CY (2001), Rules on obtaining subscriber information, pp. 17-20 See also T-CY(2018)26, Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decision and developments, p. 5-6.

[111] Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*.

[112] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB,* op. cit.

[113] See the judgment in *Big Brother Watch and Others,* op. cit., para. 356. The 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.

communications data from a communications services provider to prior review by a court or independent administrative body.[114]

The data-categorisation challenge becomes even more problematic when considering the absence in the proposed regulation of specific rules on inadmissibility for wrongly categorized data. It might therefore become possible that data collected according to the wrong procedure (e.g. without the required independent judicial validation) could still be admitted as evidence in some EU member states. A Task Force participant observed that courts in some EU countries (e.g. Belgium) will not dismiss a case 'simply because' the data has been wrongly categorized in the pre-trial phase. Indeed, rules on admissibility of evidence in criminal proceedings vary greatly across the Union, nor a clear EU legal framework of admissibility of evidence yet exists.

The e-evidence regulation proposal also foresees the introduction of new (sub)-category of 'access data' which does not match with the one provided under already existing EU legal instruments (Warken, 2018). While intended to be distinguished from traffic data, access data still remains vaguely defined compared to the other already existing categories.[115] The creation of new sub-categories of data to which different level of protections are attached appear however in tension with the proposal - made in the draft of the so-called ePrivacy Regulation[116] - to consider that "electronic communications data should be defined in a sufficiently broad and technology neutral way so as to encompass any information concerning the content transmitted or exchanged (electronic communications content) and the information concerning an end-user of electronic communications services processed for the purposes of transmitting".

Another privacy-related challenge relates to the duty to inform the data subjects whose information is being sought. Article 11 of the proposed e-evidence regulation requires service providers to take 'necessary measures' directed at ensuring the confidentiality of the order and aimed at preventing that persons affected by the order become aware that they are investigated. The Commission foresees that the secrecy of the investigative measures should be guaranteed as long as the issuing authority deems it 'necessary and proportionate to avoid obstructing the relevant criminal proceedings'. At the same time, the proposal does not require the issuing authority to include in the certificate accompanying the order any explanations justifying the necessity to keep the investigative measure secret. While it is not for the service providers to assess the necessity of keeping an Order secret, such information could indeed be valuable in order to

[114] Ibid. paras 463, 466 and 467.

[115] EDPB, Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), p. 12.

[116] Proposal for a regulation of the European Parliament and of the Council 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/2017/010 final - 2017/03 (COD).

adequately assess whether fundamental rights objections, as foreseen in the Commission proposal, should be raised by the addressee of the order.

This type of requests (so called non-disclosure orders) could potentially be issued in all criminal proceedings, and would not necessarily be restricted to cases where notification to the data subject would put life, limb or property into serious danger.[117] In case of production orders targeting subscriber and access data, as well as of preservation orders, this sort of non-disclosure orders could also be issued without prior validation by an independent judicial authority. The involvement of such authority would not necessarily entail informing the data subject of the ongoing criminal investigation, but would instead ensure an additional level of scrutiny over the necessity and proportionality of the order, as well as of the decision to maintain the secrecy of the investigative measure. Furthermore, there are no provision in the proposal that would allow the service providers (let alone the competent oversight authority in the state of execution) to require further information when deemed necessary to verify the existence of legitimate grounds justifying the issuing of a non-disclosure order.

The Commission's proposal does not specify whether the service providers' obligation to refrain from informing the data subjects applies to all orders, or just when the issuing authorities expressly require to do so (in the accompanying certificate). This last option was instead preferred by the Council, which in its general approach explicitly requires service providers to refrain from notifying the data subject, except when otherwise (expressly) indicated by the issuing authority.[118]

The restrictive approach to notification restrictions adopted by the Council becomes especially concerning in light of the draft regulation's wide scope of application *ratione persona.* Not only does the proposed measure provide a definition of 'service providers' that covers a wide range of businesses[119] but, as the EDPB noted, the non-disclosure orders foreseen by the proposed regulation could be addressed to both data controllers and processors (in the sense of the GDPR). At the same time, a secret order issued to the data processors would prevent the latter from having the possibility to notify the data controller of the existence of a production or preservation order. In this situation, however, data subjects' rights might be circumvented.

According to the GDPR, a processor only acts on the instructions given by the controller. This means that it is the responsibility of the controller to ensure the rights of data subjects are respected, and to provide them with the relevant information, including with regards to recipients of their data, for instance in the context of the exercise of their right of access. On the other hand, while the draft regulation allegedly follows a controller first principle, it does not expressly prevent

[117] European Parliament, 6th working Document (A), 01 April 2019, p, 3.

[118] See article 11(1)-(2) of the Council "Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters - general approach", Brussels, 26 November 2018.

[119] Article 2 (3) (c) of the proposed Regulation on e-Evidence.

investigating and prosecuting authorities to address requests for data (limited not only personal data subject to the GDPR) to the addressee deemed as most appropriate (including processors), regardless of the data protection rules applicable. The EDPB therefore stressed that data subjects benefitting from the application of the GDPR may not be able to exercise their rights efficiently if, as a consequence of an order served upon a processor providing services for the controller (e.g. storing data), the latter is not in a position to provide complete information to the data subject.[120]

In cases where the service provider must refrain from notifying the subject concerned by the order the draft regulation foresees an express duty for the issuing authority to inform the person whose data are being sought 'without undue delay'. And even then, the information might be delayed as long it is necessary and proportionate to avoid obstructing the relevant criminal proceedings.[121] The assessment of the necessity and proportionality to keep the order secret will be conducted exclusively by the issuing authority (in some cases represented by prosecutors), without any possibility for the country of execution to question the assessment conducted by a foreign investigating and prosecuting authority. Also, the duty to inform the suspect or accused person would only subsist as far as production orders are concerned, since the proposal does not foresee any obligation for the issuing authority to notify the data subject in case of preservations orders obliging the service providers to refrain from notification.

The so-called 'Police Directive'[122] provides a general obligation for law enforcement authorities to inform data subjects, and deviations to the principle of notification of the data subject are clearly framed as exceptions to the rule. On the contrary, in the proposed e-evidence regulation it is the opposite, since a (partial and limited) obligation for the issuing authority to notify the data subject only exists when a request is made to the service providers to refrain from informing the person whose data are being sought. This is where *the nexus between effective remedies, fair trials and the right of privacy* emerges in sharp relief.

7.3.3 Effective remedies and fair trials

The right to an effective remedy is crucial to the effectiveness of the rights bestowed upon individuals by the EU Charter and other international and regional human rights instruments, including the ECHR (Hofmann, 2014, p. 1211). The effectiveness of remedies depends, in turn, on the existence, and accessibility of remedial avenues, including both institutions and procedures

[120] EDPB, Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), p. 10.

[121] See article 11(2)-(3) of the proposed regulation.

[122] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

capable of *preventing* and *redressing* abuses related to the use of coercive powers, including in the context of criminal proceedings.[123]

As outlined in Sections 1 and 2 of this Report, the EIO Directive envisages a set of suspects' rights and guarantees aimed at ensuring compliance with Article 47 of the EU Charter. At the same time, JUD-IT research has shown that the effective delivery of these EIO protections of the rights of the defence are often subject to a number of practical and legal obstacles in many EU member states under investigation.

Ensuring access to effective remedies against fundamental rights abuses that might derive from the introduction and use of the data-gathering measures envisaged in the proposed e-evidence regulation would also become difficult in a context where there are no guarantees - for suspect and accused persons, as well as for third parties concerned - of a systematic *ex ante* involvement of independent judicial or administrative authorities in neither the state of issuing or execution. The delivery of ex ante remedies would also be hampered by the lack of a duty to inform, in a timely manner, the different categories of data subjects potentially affected by the proposed measure. These include not only the suspects directly concerned by the criminal investigation, but also third parties whose rights might be negatively affected by the investigative measures.

The possibility that information pertaining to individuals different from the suspect or accused persons are collected or preserved is intrinsic in the execution of data-gathering measures adopted in the context of a criminal proceeding. In some cases, third parties' data are collected or preserved because such information is of direct relevance for the investigation or prosecution of a crime. However, it might also happen that third parties' data are collected or preserved only incidentally, since they do not constitute the direct target of the investigative measure. Against this backdrop, allowing national data protection authorities to formally exercise the rights of data subjects 'indirectly' (as instead provided under national laws of EU several countries), and being notified when an order is issued, appears as particularly crucial.

While it is clear that specific stages of investigations may require secrecy, a system that could potentially allow a systematic exclusion of notification regarding the gathering and preservation of data of different categories of individuals fundamentally challenges not only existing EU privacy and data protection standards, but also the principle of equality of arms and the adversarial principle in criminal proceedings. The priority given to maintaining secrecy of the investigative measure (potentially until after an indictment is made), as well as late notification to the different

[123] These include: Directive 2010/64/EU on the right to interpretation and translation in criminal proceedings, Directive 2012/13/EU on the right to information about rights and charges and access to the case file, Directive 2013/48/EU on the right of access to a lawyer and communication with relatives when arrested and detained, Directive 2016/343 on the strengthening of certain aspects of the presumption of innocence and the right to be present at one's trial, Directive 2016/800 on the procedural safeguards for children and Directive 2016/1919 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings.

categories of potentially affected individuals would make it difficult to object and/or challenge its legality, proportionality and necessity of an order, especially in the early stages of a proceedings.

The e-evidence regulation clearly recognises the possibility to challenge an issuing authority's production order. Article 17(1) of the E-evidence proposal stipulates that the suspect or accused person has the "right to effective remedies against the European Production Order during the criminal proceedings for which the Order was issued". According to Article 17(3), "such right to an effective remedy shall be exercised before a court in the issuing State in accordance with its national law and shall include the possibility to challenge the legality of the measure, including its necessity and proportionality". It does, however only granted this is opportunity once the production order has already been given effect. At that point, however, it might be difficult to redress the negative effects of an unlawful or abusive order. Art. 7 of Directive 2012/13/EU on the right to information in criminal proceedings[124] guarantees access to the file covering evidence on which the prosecution is built. And yet, investigating or prosecuting authorities may be put in a position to construct a case based on evidence obtained illegally through the recourse of a secretly adopted and implemented data-gathering measure.

Furthermore, the proposal does not extend the right to seek remedies to the persons who are suspected or accused of a crime and whose data have been targeted by a preservation orders (EPOC-PRs). The right to effective remedy of third parties could in fact only be exercised only against a European Production Order. In substance, the proposal does not foresee any rights to an effective remedy in cases of European preservation orders. Third parties affected whose data are affected by preservation orders would neither be able to seek remedies.

Further problems arise if complaint mechanisms and/or appeal procedures that can be activates after the order has been issued and/or executed are designed in a way that *de facto* undermine the availability of remedies. For instance, it is concerning that the proposal does not impose upon the prosecuting authorities a clear obligation to formulate the orders so that, beside incriminatory data, they also cover information that can be used by the defence. The proposal does nor set out precisely the conditions upon which the suspects could request competent authorities the issuing of an order, and leaves the determination of such conditions to national law of the different member states. Nor does the proposal indicate which are the 'types of remedies' or reparations available to the data subjects once the latter has proved that his/her rights were abusively interfered with in the context of the data-gathering procedures under discussion. Also in this case it is left to member states the duty to specify - as a matter of national law – the ex post remedies available in case of abuses.

[124] Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, L144/1.

7.3.4 Challenges for Business

JUD-IT research has shown that 'domestic cooperation' between providers of internet and telecommunication services and national authorities of their country of establishment is generally viewed as positive in many member states. Cloud service providers and telecommunication companies have by now developed internal procedures and equipped themselves with the necessary human and technical resources to handle requests for data.

The increasing pressure to respond to direct cross-border requests for data (i.e. requests addressed directly to service providers and outside the judicial cooperation instruments provided by MLATs and the EIO directive), however, expose service providers to higher risks of being in breach of the privacy and criminal justice laws applying in the country concerned by an incoming request issued by a foreign authority.

Research conducted throughout the JUD-IT project has shown that many IT companies and cloud providers see an added value in harmonising common EU standards regulating access to electronic data for criminal investigation purposes. Such rules could reduce legal uncertainties, in particular by providing a legal basis for broader and smoother cross-border cooperation with authorities requesting data. Some companies also see the proposal as a way to define the needed safeguards for the challenges that arise when investigating or prosecuting authorities go directly to providers. A major issue that remains unresolved, however, is that initiatives aimed at making it compulsory for companies to respond to requests *vis-à-vis* the issuing authority need to ensure a higher degree of legal safeguards and guarantees so as to fully avoid potential liabilities under the criminal and data protection law of other countries under which jurisdiction they happen to operate and provide services.

The Commission proposal recognises that, in some cases, service providers have the right (but not the duty) to challenge the orders.[125] However, given the very scant information available in the certificates through which an order is transmitted to the companies,[126] in practice the effective exercise of such a right can be expected to face obstacles , especially when it comes to objections based on fundamental rights concerns. In any case, the scrutiny by a private company can only constitute an 'additional safeguard', and not a substitute of the responsibility of states, and chiefly, of their judicial and data protection authorities to protect the fundamental rights of their citizens and any person falling under their jurisdiction.[127]

Specific challenges arise when the private sector stakeholders concerned by the proposed measures are not major cloud service providers and IT companies, but small and medium

[125] See Article 14-16 of the proposed regulation.

[126] See Article 5(3) and 6(3) of the proposed regulation.

[127] Under US law, constitutional protection is instead only granted to US citizens or to subjects with a link to the US territory.

enterprises (SMEs). While high volumes of requests would only occur if a service provider has a high number of customers, there is a clear risk that these SMEs will simply lack the resources to cope directly with cross-border requests. The proposed regulation would give EU investigating and prosecuting authorities the possibility to issue Orders for a large variety of crimes, including non-serious ones (virtually for all offences when it comes to preservation orders and production orders targeting subscriber and access data). The possibility given by the proposed regulation to issue production orders targeting subscriber and access for all crimes would potentially expose small and medium enterprises in certain member states to the obligation of having to deal directly with significantly higher numbers of data requests. For SMEs, executing an order within the 10 days' deadline might also be difficult to ensure in cases where there is a lot of data to download and process in order to execute the order. Complying with the fast track procedure (6 hours timeframe) foreseen in the proposed regulation would be simply impossible for small and medium-sized service providers due to lack of in-house expertise and resources. The short time given to execute orders would furthermore run the risk of increasing pressures to comply to requests for data, without simplifying the technical processes that in practice need to be undertaken in order to retrieve the data. Representatives of SMEs potentially affected by the proposed measures also expressed concerns about their actual capacity to conduct the complex legal assessment required to raise the fundamental rights and conflict of laws objections envisaged in the Commission's proposal.

Another issue of crucial concern, especially for SMEs, relates to reimbursement of costs. Private sector representatives have been vocal in stressing that claiming costs associated with the execution of the orders before the authorities of the issuing country would be cumbersome, but could also lead to unclear and unforeseeable situations. Especially for small and medium-sized companies, it would be practically impossible to effectively navigate the rules and procedure to follow in order to obtain costs reimbursement from (potentially) 27 different issuing member states. Art 12 of the Council's general approach on the proposed regulation foresees that member states shall inform the Commission about rules for reimbursement, and that the Commission shall make them public. However, new procedural and financial hurdles are likely to arise from the decision to abandon the model currently governing cost-reimbursement under other mutual recognition schemes, where the cost related to the execution of a criminal justice measure are claimed before the authorities of the state of execution, where the addressee of the order or its legal representative are established.

Regarding providers of telecommunication services, they usually have well-established cooperation channels with the law enforcement authorities in the country where they are based. In certain countries, the creation of single Points of Contacts (POCs) on both sides makes it possible to maintain trust and smooth cooperation through secure and tested channels. While the service provider could appoint these persons as legal representatives for the purpose of receiving and executing the order under the proposed e-evidence regulation, recreating the forms of direct

cooperation established with domestic investigating and prosecuting authorities along the years is expected to be difficult. Under current cross-border judicial cooperation proceedings in the EU, the company receives orders that have been received and validated by the national authorities and judicial actors responsible for executing the requests for disclosure of data. Incoming requests are thus domesticated and consequently 'look' as if they were national investigative measures. For the telecom sector initiatives such as the proposed regulation, which would require to (potentially) deal and comply with orders issued by authorities from other 26 member states belonging to different constitutional and criminal law traditions. Such an obligation would bring new legal ad procedural challenges since it would change tested practices in areas such as verification of delivery authenticity, and the use of secure transmission channels for the handling of requests. Authentication constitutes a key issue for service providers which might become potential recipient of the proposed orders. JUD-IT research has showed the importance of ensuring clear rules that would allow for the secure identification of the issuing authorities, as well as provisions requiring the latter to send the standardised EPOCs and EPOC-PRs through a common standardised gateway.[128]

The Council general approach of December 2018 on the e-evidence proposal has envisaged a further 'downgrading of safeguards' in comparison to the original Commission's proposal. The Council text excludes any meaningful mechanism that service providers could use to raise objections against the orders based on their incompatibility with even the most basic forms of fundamental rights protection provided in the EU Charter. Several service providers are concerned that maintaining a relationship of trust with their customers would become difficult in a context where objecting the fundamental rights incompatibility (even if manifest) of the investigative is no longer permitted upon receipt of the order. For service providers challenging the orders would only become possible in the context of the subsequent enforcement phase, by the mean of invoking certain formal 'restricted grounds' of non-compliance.[129] While it is clear that private actors should not become solely responsible for assessing the legality of the investigative measures addressed to them, the possibility of addressees of the orders to raise fundamental rights concerns is critical, especially because in some cases only service providers will have the ability to identify demands that are abusive, overly broad, or inappropriate for other reasons.[130] Another point of concern relates to the modification of the notification regime to a system where notification to the data subject (or to the national data protection authorities) is only possible when exceptionally and expressly mandate by the issuing authority.

[128]Article 8 of the proposed regulation would leave issuing authorities the choice of using 'any mean capable of producing a written record' or, whereas available, pre-established channels of communication with the service providers.

[129] Recital (45) of the Council General Approach.

[130] Microsoft's Response to the Council Position on the Proposed e-evidence Regulation, January 2019, p. 5

The proposal made in the Council's general approach to add a pecuniary sanction of up to 2% of the overall annual turnover in cases of non-compliance undermines any real possibility for companies to raise timely objections upon receipt of the orders, even when they should or could do so. The general approach indicates that the competent enforcing authority should graduate the entity of the sanction upon the assessment of certain factual circumstances such as nature and gravity of the 'breach' and factors such as voluntariness or negligence at the basis of the addressee non-compliance. And yet, a large margin of discretion is left upon enforcing authorities in this regard. For instance, the executing authority might still decide to impose a sanction to 'micro-enterprises' that - due to lack of personal resources - fail to comply with the 6 hours deadline of an order issued in an emergency case and received outside normal business hours, if the data is not transmitted 'without undue delay' upon expiration of the deadline.[131]

Furthermore, the ratio underlying the sanction proposed by the Council in its general approach appears different from the one characterizing the 4% turnover (or €10 million) penalty linked to violations of the GDPR's basic principles for data processing,[132] data subjects rights,[133] or in case of non-compliance with an order by a supervisory authority.[134] The sanctions foreseen in the GDPR are directed at ensuring the enforcement of EU data protection standards worldwide while preventing abuses. By contrast, the sanctions foreseen in the Council general approach on the e-evidence regulation are directed at sanctioning instances of non-compliance (even when legitimate) with investigative measures which, by design, interfere with fundamental rights of data subject protection. Upon reception of an Order, companies would be put in the position to execute an order even when they should have not done so.

[131] Recital (45a) of the Council General Approach.

[132] Art. 5, 6, 7, and 9 of the GDPR.

[133] Art. 12-22 of the GDPR.

[134] Art. 83.6 of the GDPR.

8. Concluding remarks and policy options

The JUD-IT project has shown that under EU criminal law, efficiency can only be achieved where 'speed' in gaining access to data is commensurate to respect of the rule of law and fundamental rights standards enshrined in the EU primary and secondary norms governing criminal justice cooperation and the gathering evidence, including in digital form.

EU criminal justice and data protection rules and standards apply to investigative measures emanating from member states' 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 operating under EU law. Furthermore, they are binding upon the service providers holding the data sought. Fundamental principles of law deriving from national constitutional traditions (of EU and third countries) must also be considered to guarantee that data are collected lawfully across borders and can be admitted as evidence before the courts.

Data-gathering tools for criminal justice purposes must function in ways that prevent the multi-level conflicts of laws that typically derive from extraterritorial enforcement of criminal jurisdiction. From an EU perspective, such conflicts can be avoided only through effective judicial oversight over the issuing *and* execution of cross-border criminal justice measures. Preservation of trust in the EU criminal justice system is rooted in the principle of separation of powers, and practically ensured through day-to-day cooperation between the competent judicial authorities of the different countries concerned by a cross-border data-gathering measure.

Across the EU, the judicial authorities responsible for respectively requesting, validating, and executing investigative measures targeting electronic information differ depending on factors such as the specific type of data sought, whether the measure involves preservation or production of data, but also based on the categories of persons affected, as well as the specific stage of the proceedings in which such measures are to be executed. Different national rules apply to the conditions justifying access to information for criminal justice purposes, as well as to the specific procedural safeguards applying to law enforcement requests for data sought in criminal proceedings.

The systematic involvement of competent judicial authorities in the country of issuing *and* execution of a criminal justice decision is a crucial precondition for mutual understanding and trust. On the one hand, it ensures that requests for electronic information are lawful, necessary and proportionate. On the other hand, it allows for the appropriate assessment of whether legitimate and indeed obligatory grounds exist to refuse the implementation of another country's data-gathering measure.

Only judicial authorities meeting precise independence standards possess the institutional prerogatives and professional capacity to appropriately scrutinise the legality, necessity, and

proportionality of a criminal justice decision, but also to decide not to recognise or execute of another member state's criminal law enforcement measure. Member states' judicial authorities are in fact those with whom the duty to protect and enforce fundamental rights and freedoms of concerned individuals, including both suspects and accused persons, and data subjects' rights arising from EU law primarily lies. While private companies might be well-placed to raise certain fundamental rights concerns (e.g. those emerging from highly technical assessments), they should not become responsible for ensuring the fundamental rights compliance of law enforcement measures directed at the collection of data for criminal justice purposes.

A clear legal framework is needed by suspects and accused persons to effectively defend their rights and exercise their prerogatives at all stages of criminal proceedings. Data subjects must also be protected against unlawful interference, and their rights restricted or interfered with by law enforcement actors only in accordance with the law, and to the extent that is necessary and proportionate in a democratic society.

In light of the above, a number of policy options emerge as possible ways forward to: improve the uses currently made of currently existing instruments of judicial cooperation for evidence gathering in criminal matters, and tackle related implementation challenges, and; address challenges identified in relation to the e-evidence proposal, and its compatibility with the rules and standards governing criminal justice cooperation within the EU, and in relations with third countries.

8.1 Enhancing already existing judicial cooperation instruments

Within the EU, the EIO offers a valuable tool for member states to cooperate in the field of evidence gathering in criminal proceedings. This mutual recognition instrument can increase the level of judicial scrutiny and protection of cross-border measures that, in a purely domestic context, could be issued and executed without prior judicial validation. While more time is required for the EIO to 'fully flourish', additional efforts could and should be made to address existing implementation gaps and operational and technical shortcomings.

8.1.1 Practitioner's guidance and specialised training

Across the EU, a serious problem that has been identified is that practitioners are often 'lost in translation' due to the different legal terms and notions used across various countries. The compilation of a 'glossary' for practitioners, with basic explanatory concepts, comments and links to legal provisions related to other countries, could help resolve this issue. If there is some streamlined guidance, practitioners would be able to navigate obstacles much more easily.

More efforts should be devoted to promoting systematic exchange of practical experiences among judicial actors and legal practitioners and developing guidelines to follow when issuing or executing EIOs requiring preservation or production of data. Specialised trainings should be promoted at the

transnational level to improve competent judicial authorities' mutual understanding of reciprocal administrative practices and challenges faced in issuing and/or executing EIOs. These initiatives could also help raise practitioners' awareness of the possible ways in which the EIO can be used to access different categories of data sought for criminal justice purposes within the EU.

Regarding member states' cooperation with the US, further support should be given to practical measures directed at improving cooperation and mutual understanding between member states and US judicial and diplomatic authorities, including through the organisation of technical dialogues, training, and exchanges of information and promising practices on applicable rules and procedures related to the issuing and treatment of MLA requests in a transatlantic context. More human and financial resources could be allocated to support judicial authorities in the formulation of 'quality requests'.

To date, only a very few member states have appointed specialised liaison magistrates in Washington, despite the fact that their deployment can facilitate the processing of their countries' MLA requests in US, and in particular ensure that they take US legal standards into due account, most notably that of 'probable cause'. Guidelines on how to issue 'emergency requests' for data held by US companies could also be developed in cooperation between the EU and the US, and made available to practitioners across the Union.

8.1.2 Secure and swift channels of communication

The EU should maintain and increase support for the development of tools aimed at facilitating judicial cooperation and communication, including through the e-Evidence Digital Exchange System, which is based on the e-CODEX platform and designed to provide a channel for digital exchanges of EIOs and replies between EU judicial authorities. Further development of these new channels for transmitting EIOs could streamline and speed up cooperation and exchange of data and evidence between the competent authorities of member states in a trusted and secure way.

The possibility to also use the e-CODEX platform to automatically translate EIOs issued or received could significantly reduce administrative burdens. In the meantime, prosecution offices and courts of member states participating in the EIO could be encouraged to award a contract (following a public tender) to private translation firms, under the terms of which a minimum number of pages per month, and even per day in urgent cases, shall be translated on demand. This practice would release judicial authorities from the burden of translation while accelerating the whole process.

It could be envisaged the establishment of a 24/7 online support service capable of providing relevant information on EIOs submission and follow-up procedures, including information on expected timelines for execution could also be considered. Taking due account of the different rules, procedures, and categories of actors involved in the MLAT process, similar solutions could also be explored to improve secure communication and transmission of requests with and from

the US. Guidelines could also be developed to help private companies (especially SMEs) to learn how to deal with different types of cross-border requests for data.

8.1.3 Monitoring and ensuring effective judicial oversight

EU countries should ensure that judicial scrutiny over the issuing and execution of EIOs is not only formal, or just amounting to an automatic approval of police requests for data. Issuing authorities should not use the EIO to bypass judicial checks by authorities different from the one issuing the request or investigating the case, when their involvement is foreseen in equivalent domestic procedures. These practices run counter to the rule according to which issuing member states shall ensure that legal remedies equivalent to those available in a similar domestic case are applicable to the investigative measures indicated in the EIO.

JUD-IT research has also shown that differences still exist in the ways in which EIO treat incoming requests for data, as compared to domestic ones. Some EU countries apply an additional level of scrutiny over EIOs received from other member states. Such cases shall be better monitored to verify whether they effectively undermine the EIO attempt at moving beyond the MLATs system within the participating member states.

8.1.4 Effective protection of defence rights

Defendants should be effectively empowered to require the issuing of an EIO, "within the framework of applicable rights of the defence in conformity with national criminal procedure". Legislative gaps at the national level should be addressed by those EU countries that did not include the corresponding EIO Directive provision in their national legislation.

In parallel, efforts should be made to tackle the lack of knowledge among defence lawyers about the possibility to use this instrument. Increasing legal practitioners' awareness about the existence of the instrument and of the ways and circumstances in which it can be used is especially important to effectively guarantee the principle of equality of arms in mutual recognition proceedings. More research should be conducted to foster a better understanding of how to deliver effective defence rights through improved access to a lawyer and legal aid in the different phases of cross-jurisdictional investigations that involve use of data.

8.2 Aligning the e-evidence proposal with the EU rule of law, criminal justice and data protection standards

Several options could be explored to address the open questions that emerge when analysing the proposed e-evidence regulation in light of EU primary and secondary law.

8.2.1 Direct contact between competent judicial authorities

Member states authorities could be allowed to issue preservation orders and address them directly to service providers across borders, prior validation by an independent administrative body or judicial authority and subject to strict ex-ante necessity and proportionality assessment.

Effective judicial oversight over the issuing *and* execution of production orders should be always ensured, regardless of the type of data sought. The possibility should exist for the executing authority to verify that the issuing of the EIO is necessary and/or proportionate, and to consult the issuing authority on the importance of executing the preservation order, in line with EIO rules. Grounds for non-recognition and non-execution should be foreseen, in line with existing EIO rules.

8.2.2 Restricting application of the new instruments ratione materia

Given the fundamental rights-sensitive character of the proposed measures, considerations should be given to the possibility to limit the scope of application of the proposed regulation to certain types of crimes.

The use of production or preservation orders could be restricted to the investigation or prosecution of offences capable of attracting a maximum custodial sentence of at least 3 years or more. A three-year threshold for all orders (and not just for production orders targeting content or transactional data) would limit the scope of the instruments to more serious crimes, without excessively limiting the possibilities of its use by practitioners. The use of orders could also be allowed for the purpose of investigating or prosecuting offences for which evidence is typically available only or mostly in electronic form. For this purpose, a list of specific harmonised offences could be drafted and annexed to the e-evidence regulation.

8.2.3 Enhancing rights of suspects and accused persons, and of data subjects

Restrictions to the rights to be informed should be limited to situations where maintaining secrecy is necessary and proportionate to the need of protecting sensitive law enforcement information.

Exceptions to investigating or prosecuting authorities' notification duties should not be formulated in an excessively broad way which systematically prevents the exercise of criminal justice (fair trials) and data protection (fair data processing) rights in practice. The practical exercise of the right of data subjects to be informed could be enabled, for instance, through the involvement of trusted third parties (e.g. national data protection authorities).

The proposed regulation could include provisions detailing the conditions upon which the suspects could request competent authorities the issuing of the envisaged investigative measures. To ensure the 'equality of arms' principle in mutual recognition proceedings, the regulation should not only generally envisage the possibility for defence lawyers to request the issuing of production and preservation orders, but also determine the conditions and circumstances in presence of

which such requests could be made, and the specification of some criteria for their assessment by competent authorities in the issuing country.

The draft regulation could include provisions establishing that when the *ex-post* review of the way in which the data were gathered reveals that certain data were obtained unlawfully, such information should not be admissible as evidence. The proposal could also directly indicate the types of remedies or reparations available to the data subjects once the latter has proved that his/her rights were abusively interfered with in the context of the data-gathering procedures under discussion.

Provisions similar to those included in the EIOs related to *ex-ante* and *ex-post* judicial remedies should be included, in particular to clarify that remedies ensured in the country of issuing should be without prejudice to the ex-ante and ex-post guarantees of fundamental rights in the executing state.

8.2.4 Legal clarity for private companies

The scrutiny of orders received by a private company should only be intended as providing an 'additional safeguard', which is not a substitute for the responsibility of EU member states to protect the fundamental rights of their citizens or of any subject falling under their jurisdiction.

More precise provisions specifying the exact grounds, conditions and circumstances upon which companies might raise objections against a received order could be included in the e-evidence regulation. Further clarifications could be provided about the conditions and circumstances in presence of which an order should be considered as manifestly abusive in light of the EU Charter. The possibility to seek clarifications or raise objections should also be given when fundamental rights risks, even if not manifest, are identified with regard to the received orders. More information should be included in the certificate accompanying the order to allow the addressee of an order to assess whether a legitimate ground of non-compliance subsist.

Financial sanctions against cases of non-compliance need to be carefully regulated and subject to stricter necessity and proportionality criteria. The introduction of financial sanctions in the regulation should not undermine any real possibility for the companies to raise legitimate objections to the orders.

The proposed regulation should ensure that providers are not placed in a worse position to challenge unlawful or otherwise inappropriate orders than they would be under domestic law. Legal avenues available to providers under domestic law to challenge orders should be at least equal to those currently indicated in a European Investigation Order.

8.2.5 Preventing future conflicts of law in a transatlantic context

Key standards stemming from the Court rulings and concerning conditions ensuring the legality of data transfer to third countries will need to be taken carefully into account In the negotiations of a new EU-US Agreement for cross-border access to electronic information in criminal proceedings.

Transfer of personal data from the EU to the US should be made conditional on verification that the US offers an adequate (i.e. equivalent) level of data protection to the one granted under EU law, read in light of the Charter. To date, adequacy decisions currently in place with the US do not cover data exchanges in the law enforcement and criminal justice sector. The legal basis for the exchange data sought for criminal justice measures is currently provided by the EU-US MLA agreement, which require the involvement of independent oversight authorities responsible for reciprocally verifying that the standards and conditions are met for each data transfers. The Umbrella Agreement also applies.

A new agreement between the US and the EU on the exchange of electronic data in criminal proceedings should foresee the involvement of the judicial authorities of both parties as soon as possible in the process of gathering electronic data, and ensure that these authorities would have the possibility to review the compliance of the orders with fundamental rights and raise grounds for refusal.

Any future EU/US agreement on cross-border data gathering for criminal justice purposes will need to ensure reciprocity and avoid discrimination based on nationality. There would be no reciprocity in a context where EU authorities still needed to meet probable cause standards in order to obtain US citizens' data held by US companies, while the US would be granted the power to directly compel companies falling under EU jurisdiction to disclose and transfer any type of data (i.e. content and non-content including, it seems, when such data pertain to EU citizens), without obtaining prior authorisation of an EU member state court.

The new agreement should provide the only channel for issuing and executing requests at the transatlantic level. Data-gathering measures by law enforcement authorities should not be served outside the legal framework of the agreement.

References

Armada, I. (2015), "The European Investigation Order and the Lack of European Standards for Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution?", *New Journal of European Criminal Law*, 6(1), 8–31.

Bachmaier Winter, L. (2019), "Bypassing or Intensifying the Dialogue between Courts ? The Impact of Melloni at the National Level", in V. Mitsilegas, A. Di Martino and L. Mancano, *The Court of Justice and European Criminal Law: leading Cases in a Contextual Analysis*, Hart Publishing, pp. 404-420.

Bárd, B. (2018), "Saving EU Criminal Justice Proposal for EU-wide supervision of the rule of law and fundamental rights", CEPS Papers in Liberty and Security No. 2018-01, April.

Bárd, P. and W. van Ballegooijk (2019), "The Effect of the CJEU Case Law Concerning the Rule of Law and Mutual Trust on National Systems", in V. Mitsilegas, A. Di Martino and L. Mancano, *The Court of Justice and European Criminal Law: leading Cases in a Contextual Analysis*, Hart Publishing, pp. 455-468.

Carrera, S. and V. Mitsilegas (2017), *Constitutionalising the Security Union: Effectiveness, Rule of Law and Rights on countering Terrorism and Crime*, CEPS Paperback, CEPS: Brussels.

Carrera, S., G. González Fuster, E. Guild and V. Mitsilegas (2015), *Access to Electronic Data by Third-Country Law Enforcement Authorities*, CEPS Paperback, CEPS: Brussels.

Docksey, C. (2018), "Case Note no. 3. Opinion 1/15, Canada-EU PNR", in JUD-IT Compilation of Case Notes, October.

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.

Heard, C. and D. Mansell (2011), "The European Investigation Order: Changing the Face of Evidence-Gathering in EU Cross-Border Cases", *New Journal of European Criminal Law*, 2(4), 353–367.

Hofmann, H. CH (2014), "Article 47. III Specific Provisions (Meaning) (a) context", in S. Peers, T. Hervey, J. Kenner and A. Ward, *The EU Chart of Fundamental Rights, A Commentary*, p. 1211.

Lenaerts, K. (2015), "The Principle of Mutual Recognition in the Area of Freedom, Security and Justice", Paper presented in the occasion of the Fourth Annual Sir Jeremy Lever Lecture All Souls College, University of Oxford, 30 January.

Lenaerts, K. (2017), "La Vie Après L'Avis : Exploring teh Principle of Mutual Recognition (Yet Not Blind) Trust", *Common Market Law Review*, 54, pp. 805-840.

Mitsilegas, V. (2018), "The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence", *Maastricht Journal of European and Comparative Law*, 25(3), 263–265.

Mitsilegas, V. (2019), "Resettting the Parameters of Mutual Trust: From Aranyosi to LM", in V. Mitsilegas, A. Di Martino and L. Mancano, *The Court of Justice and European Criminal Law: leading Cases in a Contextual Analysis*, Hart Publishing, pp. 421-436.

Mitsilegas, V. and N. Vavoula (2018), "The centrality and characteristics of privacy in the context of transnational criminal investigations", JUD-IT Concept Note.

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

Stefan, M. and G. González (2018), "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", CEPS Liberty and Security Series, CEPS, Brussels.

Van Ballegooij (2015), *The Nature of Mutual Recognition in European Law: Re-Examining the Notion from an Individuals Rights Perspective with a View to its Further Development in the Criminal Justice Area*, Intersentia, Cambridge: United Kingdom.

Wahl, T. (2019), "Council Pushes for E-Evidence Law, EP Applies the Brakes", *Eucrim news*, 18 February.

Warken, C. (2018), "Classification of Electronic Data for Criminal Law Purposes", *Eucrim,* Issue 4/2018.

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, Resources 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)