Cross-border data access in criminal proceedings and the future of digital justice

Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic

Report of CEPS and QMUL Task Force

Rapporteurs:
Sergio Carrera
Marco Stefan
Valsamis Mitsilegas

CEPS

Queen Mary University of London

Cross-border data access in criminal proceedings and the future of digital justice

Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic

---

Report of a CEPS and QMUL Task Force

Sergio Carrera
Marco Stefan
Valsamis Mitsilegas

Centre for European Policy Studies (CEPS)
Brussels
October 2020

The Centre for European Policy Studies (CEPS) is an independent policy research institute based in Brussels. Its mission is to produce sound analytical research leading to constructive solutions to the challenges facing Europe today. This Task Force report has been drafted by Sergio Carrera, Marco Stefan and Valsamis Mitsilegas. The opinions expressed in the report are exclusively of the authors, and do not in any way reflect the position or views of any Task Force member.

Sergio Carrera is Senior Research Fellow and Head of the Rights and Security Unit at the Centre for European Policy Studies (CEPS); Part-Time Professor at the Migration Policy Centre (MPC), European University Institute (EUI) and Visiting Professor at the Paris School of International Affairs (PSIA), Sciences Po. Marco Stefan is Research Fellow at CEPS. Valsamis Mitsilegas is Professor of European Criminal Law and Global Security and Deputy Dean for Global Engagement (Europe) at Queen Mary University of London.

ISBN 978-94-6138-780-6

CEPS
Place du Congrès 1, B-1000 Brussels
Tel: 32 (0) 2 229.39.11
e-mail: info@ceps.eu
internet: www.ceps.eu

Contents

List of Tables

EXECUTIVE SUMMARY

Gathering data across borders while preserving the integrity of EU criminal justice and data protection acquis

- Over the years, the EU has equipped itself with a set of intra-EU, and international cooperation instruments allowing judicial authorities to gather and exchange different categories of data sought as evidence in criminal proceedings and held by service providers across borders.
- The EU framework of judicial cooperation in the field of cross-border evidence gathering is based on a system of mutual 'peer review' of criminal justice decisions. Such a system is designed to ensure the coherent and effective application of the EU criminal justice and data protection acquis and, at the same time, to preserve states' sovereignty and constitutional integrity.
- The systematic ex ante involvement of competent judicial authorities in the country of issuing as well as in the country of execution of a cross-border data-gathering measure is essential to maintain trust within an EU criminal justice area based on the rule of law.
- Judicial authorities in the executing state are responsible for verifying that foreign criminal justice measures do not translate into an unjustified infringement of individuals' rights and freedoms. The correct application of the so-called EU procedural rights acquis, as well as the delivery of remedies in cross-border criminal proceedings relies upon judicial control and the intervention of competent authorities in both the issuing and executing country.
- Reciprocal judicial scrutiny of cross border data-gathering measures constitutes a key legal certainty factor and must be upheld in judicial cooperation between EU countries. An equivalent (if not higher) level of judicial scrutiny must by extension apply to criminal justice and law enforcement measures originating from third countries, to which the principle of mutual (but not blind) trust does not apply.
- Only judicial authorities which are insulated from both political interests and private or commercial considerations can be responsible for verifying that foreign countries' data-gathering measures are effectively compatible with EU legal standards. Service providers, which are private companies, are neither legitimated nor competent to perform such an assessment, which is and should remain a prerogative of states' judiciaries.
- Conflict of laws can only be exacerbated by instruments that promote the direct and unmediated extraterritorial enforcement of criminal jurisdiction. This is especially true when such instruments are used by authorities operating in different criminal justice systems, with different traditions.

Instruments of intra-EU and external cooperation, and the digitalisation of EU criminal justice

- Within the EU, cross-border cooperation under the European Investigation Order (EIO) is gradually improving, with national authorities becoming increasingly acquainted with this mutual recognition instrument. In urgent cases, real-time cooperation between judicial authorities in the issuing and executing states can be facilitated through Eurojust and the judicial authorities at the National Desks.
- The EIO system guarantees that investigative measures are subject to a double layer of judicial protection. The conditions for access to electronic information are governed by the law of the issuing state and the law of the executing state (thresholds, e.g. serious offences or catalogue offences, or rules protecting professional secrecies).
- The involvement of judicial authorities in the executing country ensures legal certainty for the service providers holding data. The addressee of the order can trust that the investigative measures have been adopted following the right procedures. It does not have to invest time and efforts in verifying whether the EIO has been issued or validated by an authority that is competent to do so.
- There is no quantitative or qualitative evidence showing that EIO procedures take too long and are ineffective for the purpose of collecting different categories of electronic information across borders. Neither is there consensus among prosecutors or judicial authorities that new instruments of intra-EU judicial cooperation for cross-border data gathering are urgently needed.
- However, the establishment of a single EU portal of electronic communication and transmission of digital EIOs between judicial authorities could significantly speed up and streamline the exchange of information and documents within the EU criminal justice area. An EU-level platform allowing competent judicial authorities to communicate and exchange data in a secure and trusted manner is needed to complement already existing national systems, and to improve cross-border judicial cooperation for cross-border gathering and exchange of evidence within the EU.

Instruments of external cooperation and international developments

- At a transatlantic level, the CJEU's recent pronouncement in the Schrems II case laid bare the incompatibility of US government data processing practices with EU fundamental rights guarantees.
- To be legally viable and 'court-proof' EU international cooperation instruments enabling cross-border transfers of data must provide for effective – substantive and procedural – safeguards. The effectiveness of these safeguards depends, in turn, on their ability to ensure that access to data by third countries' authorities does not translate into unjustified interference with the fundamental rights of persons whose personal data are, or could be, transferred from the EU to a third country, and most notably to the US.
- At the transatlantic level, the standing EU legal basis for the collection and transfer of electronic information sought for criminal justice purposes is the MLA Agreement with the

US. This subjects US requests for data to the judicial scrutiny of competent member state authorities, ensuring that the rights of individuals are protected in line with EU and national standards.

- Companies providing services in the EU and receiving a direct US law enforcement cross-border data gathering measures are exposed to risks of conflicts with the General Data Protection Regulation (GDPR). At the same time, challenging US data-gathering measures issued as a result of the CLOUD Act appears very difficult in practice. This piece of legislation significantly restricts the circumstances under which an 'obliged entity' can actually file a motion to quash or modify the SCA warrant, and only allows for an order to be modified or quashed if it is in the interests of US justice.
- The CLOUD Act executive agreements are designed to significantly extend the extraterritorial outreach of US law enforcement authorities over non-US companies. They do so in a non-reciprocal way (to the advantage of the US), introducing differential treatments and levels of safeguards based on criteria such as nationality or place of residence of targeted individuals (to the disadvantage of non-US citizens or residents).
- Member states' participation in international negotiations of the Second Additional Protocol to the Budapest Convention meanwhile constitutes a risk for the coherent application of EU law. The Protocol envisages the introduction of cross-border production orders that could be issued not only by EU member states, but also by third countries subject to very different criminal-law and data-protection standards. Such measures would seriously affect the scope of EU law in areas where the EU has already set its own standards and adopted legislation.

The e-evidence proposal

- The e-evidence proposals prioritise a data-driven law enforcement approach to criminal investigations. Rather than promoting cooperation (based on mutual trust and direct dialogues) between judicial authorities operating under different criminal justice systems, these initiatives are directed at enabling quasi-direct cross-border law enforcement access to data held by private companies abroad.
- To a large extent, the e-evidence rules proposed by the Commission were designed to solve a longstanding EU-US policy issue, and in particular to address challenges faced by member states' authorities in securing access to different categories of data held by US companies providing cloud and internet services in the EU.
- The introduction of an EU framework on direct public-private cooperation is intended to tackle risks of 'legal fragmentation' linked to the multiplication of different national approaches to cross-border (and most notably, transatlantic) data-gathering outside existing instruments of judicial cooperation. At the same time, it is intended to solve a financial issue (i.e. the need for countries to deploy adequate resources to deal with high numbers of incoming requests) by the mean of outsourcing - from states to private companies - the responsibilities (and associated costs) related to the execution of cross-border data gathering measures.

- In a context where processes of rule of law deterioration are accelerating in several EU countries, and where the adequacy of third countries legislation and practices on data-processing by law enforcement authorities are found incompatible with EU fundamental rights standards, there is a serious need for a thorough reassessment of the necessity and appropriateness of the proposed rules on e-evidence.
- None of the different proposals advanced by the EU institutions on the e-evidence file would guarantee a systematic and/or meaningful involvement of the member state of execution (nor of the affected member state). To effectively qualify as a form of judicial cooperation satisfying EU fair-trial standards in the criminal justice domain a measure must guarantee the review and express validation of foreign data requests by the competent authorities in the executing country. Limiting judicial cooperation for evidence gathering in criminal matters to a system of 'mutual notification' of cross-border investigative measures is in not line with EU and member states' constitutional requirements on transnational criminal jurisdiction enforcement and effective judicial protection.
- The lack of systematic and/or meaningful involvement of competent oversight authorities in the country of execution or in the affected state limits the right to an effective judicial remedy. This limitation would further increase the difficulty that individuals currently face in accessing judicial remedies in cross-border criminal proceedings. Without the opportunity to seek remedies in the country of execution, there is a risk more appeals against companies through civil law, which do not qualify as effective remedies in criminal justice.
- Making it easier for investigating and prosecuting authorities to issue cross-border data-gathering orders is likely to lead to a greater administrative burden on national judicial systems, with judicial authorities being potentially exposed to large numbers of data requests for review. There will be more time pressure on criminal justice oversight actors (i.e. courts and judges) which, in turn, risks seeing their capacity to effectively carry out an independent and impartial review of the proposed measure (in both the issuing and executing country) undermined. Furthermore, it is not yet clear how high volumes of 'raw' data obtained will be dealt with.
- Several service providers are concerned by the prospect of having to support the high costs associated with the practical execution of a potentially high volume of orders, while at the same time being obliged to claim and seek the reimbursement of costs in the country of issuing (i.e. in a country which is different from the one where they are established or provide their services).
- Given the high numbers of service providers across the EU, and the difficulties that would derive from a new obligation to deal with orders originating from 27 different member states governed by different criminal justice systems, new and largely unexplored challenges are likely to derive from the direct interconnection of law enforcement authorities with service providers in another EU member states.

- A new EU instrument allowing members states' judicial authorities to order the disclosure of content of electronic communication data directly from US service providers would not prevent conflicts of law and jurisdictions at the transatlantic level. At the same time, EU law-making institutions cannot disregard recent CJEU pronouncements stressing that EU law does not allow data to be directly transferred to third countries that do not guarantee a level of fundamental rights protection that is essentially equivalent to the one ensured under the EU legal acquis, read in light of the EU Charter of Fundamental Rights.

INTRODUCTION

Over recent years, one question has occupied the centre stage of the EU and international policy debate on criminal justice: does the increasing use of information and telecommunication technologies, and the digitalisation of everyday social and economic interactions, mean new rules and instruments are needed for the cross-border gathering and exchange of evidence in criminal proceedings?

Today, providers of internet, cloud and electronic communication services hold information that is extensively sought and used for detecting, preventing, investigating and prosecuting various types of crime, regardless of whether they are committed through the internet or in the offline world. The data held by private companies play an increasingly central role in contemporary criminal law enforcement efforts. This is true regardless of whether it is 'basic subscriber information' or IP addresses identifying the user of a specific email or social media account, 'traffic data' providing circumstantial insights (e.g. time and location), or the actual content of electronic communications.

Authorities investigating and prosecuting crime have a growing reliance on cross-border data (i.e. electronic information which is stored abroad or controlled by companies that are subject to foreign jurisdictions). Increasing demands for data have led the way to different proposals for reforms of the existing EU and international framework of judicial cooperation for cross-border collection and exchange of evidence in criminal matters.

Recent years in particular have seen the proliferation of different policy and normative initiatives developed at the EU, transatlantic and international levels. The aim of these initiatives is to create a new operational framework for cross-border data gathering that would allow state authorities to address orders requiring the production and/or preservation of data directly to providers of cloud, internet and telecommunication services in another jurisdiction.

Calls for new tools that enable unilateral cross-border access to data based on mandatory public-private cooperation have largely been justified on the grounds that existing judicial cooperation instruments – including both mutual legal assistance treaties (MLATs)[1] and, within the EU criminal justice area, the European Investigation Order (EIO)[2] – are ill-suited to the current data-gathering needs of investigating and prosecuting authorities.

[1] Available MLA instruments for intra-EU cooperation include the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters and its Protocols ('1959 MLA Convention'), the Convention Implementing the Schengen Agreement, and the 2000 Convention on Mutual Legal Assistance in Criminal Matters between the Member States ('2000 EU MLA Convention') and its Protocol. At the international level, the EU has concluded mutual legal assistance treaties (MLATs) with the US and Japan.

[2] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

To date, however, there has been a lack of quantitative and qualitative evidence showing that available instruments are ineffective, or less successful than direct cooperation with foreign service providers. On the contrary, serious doubts exist as to the added value of new forms of cross-border data gathering through mandatory public-private cooperation, in terms of legal certainty and effective judicial cooperation.

In fact, it appears that demands for smoother, faster, and broader cross-border access to data are the expressions of a policy agenda that prioritises law enforcement and data-driven policing at the expense of the correct functioning of a rule of law-oriented cooperation between judicial authorities operating under different criminal justice systems.

Within the EU, the development of measures enabling cross-border law enforcement access to digital information held by private companies was included among the objectives of the EU Agenda on Security.[3] The Agenda, which set forth the strategic framework for the EU's work on internal security, was developed under the lead of the European Commission's Directorate General for Migration and Home Affairs (DG HOME). It called for a new approach to "law enforcement in the digital age" and envisaged in particular the establishment of "public-private partnerships to structure a common effort to fight online crime".[4]

Since then, the establishment of such partnerships has been the Commission's preferred policy option to "improve criminal justice in the cyberspace".[5] A set of EU normative proposals[6] has consequently been presented by the Commission to qualify orders compelling foreign service providers to produce or preserve data, as a 'new form' of judicial cooperation in criminal matters.

The Commission justified these new EU data-gathering instruments on the grounds that some EU member states – acting unilaterally and outside the EU legal framework – already created similar tools (i.e. production and preservation orders) at the national level.[7] Furthermore, the Commission claimed that new European production and preservation orders were necessary because it was impossible for state authorities (within and outside the EU) to deploy the human and technical resources needed to process the increasing numbers of data requests coming

[3] 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, Strasbourg, 28 April 2015.

[4] Ibid. p. 20.

[5] Council of the European Union (2016), Council conclusions on improving criminal justice in cyberspace, Luxembourg, 9 June 2016.

[6] European Commission (2018), Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Strasbourg, 17 April2018; and European Commission (2018), 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, COM(2018) 226 final, Strasbourg, 17 April 2018.

[7] European Commission (2018), Commission Staff Working Document 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, Brussels, 17.4.2018, hereafter 'the Impact Assessment'

through traditional channels of judicial cooperation. The choice was thus made to establish a new operative framework under which the responsibility (and associated costs) of executing cross-border data-gathering measures would be outsourced from states to private companies.

The establishment of a framework for direct cross-border gathering of data held by private companies abroad has been a longstanding priority of the United States. In 2018, the US introduced the 'Clarifying Lawful Overseas Use of Data Act' – better known as the CLOUD Act[8] – to solve the dispute underlying the case of *Microsoft Ireland v Department of Justice*.[9] On the one hand, the CLOUD Act intends to provide a domestic legal basis for US authorities' exercise of criminal jurisdiction over US service providers holding data in another country or operating abroad (including in the EU). On the other hand, the CLOUD Act calls for 'executive agreements' that allow the competent authorities of one signatory party to directly order the production, preservation and wiretapping of data held or controlled by service providers under the jurisdiction of the other signatory party.

The introduction of new international rules on cross-border cooperation with service providers has also been promoted in the context of the international negotiations coordinated by the Council of Europe (CoE) Cybercrime Committee (T-CY). The Committee is currently drafting the text of a Second Additional Protocol to the CoE Budapest Convention on enhanced international cooperation on cybercrime and electronic evidence (also as known as the Budapest Convention). The envisaged Protocol would support the development of a multilateral framework providing a large number of countries (not limited to state parties of the Council of Europe) with broader opportunities for unilateral cross-border gathering of data.

However, these different initiatives (EU, US and international) are difficult to reconcile with the substantial and procedural safeguards, and rule of law framework, that underpin internal and external EU criminal justice cooperation, and which govern the collection, transfer and use of data for these purposes.

The widespread use of information and communication technologies significantly and increasingly exposes people's private lives, as well as their liberties, freedoms and rights, to the investigative and prosecuting state machineries. Interference with these rights, liberties and freedoms – which are granted a high level of protection under EU primary and secondary law – may be justified for the legitimate purpose of combating crime, but only to the extent that it is necessary and proportionate "in a democratic society".[10]

---

[8] CLOUD Act, S. 2383, H.R. 4943.

[9] *Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp*. 3. 15 F. Supp. 3d 466 (S.D.N.Y. 2014). The case originated in Microsoft's refusal to execute a warrant received directly from US authorities, which requested that Microsoft Ireland disclose some data stored in the EU. The US Department of Justice argued that its warrant authority under the Stored Communication Act compelled US-based companies to turn over the requested data, regardless of where the latter were stored. Microsoft, by contrast, maintained that this authority did not extend to data located outside US territory. The company consequently challenged the US warrant's power to reach overseas data. The case, which had been pending appeal before the US Supreme Court, was ultimately dismissed.

[10] See European Court of Human Right (2020), Factsheet – Personal data protection, May 2020. Available at https://www.echr.coe.int/documents/fs_data_eng.pdf.

Existing instruments of EU and international cooperation have been designed to reconcile the aim of effectively investigating and prosecuting crime with the equal imperative to ensure that investigating and prosecuting authorities' actions (including demands for electronic information) are subject to effective judicial checks. These instruments foresee the systematic ex ante involvement of competent judicial authorities in the countries of issue *and* execution of a cross-border data-gathering measure. The aim is to ensure that the preservation or production of data follows the appropriate legal processes and is supervised by the competent oversight bodies in the countries of issue and execution.[11]

The necessity of ensuring effective ex ante judicial scrutiny over investigating and prosecuting authorities' actions ultimately depends on the principle of separation of powers. Only the authorities representing the judicial power are insulated from political interests, as well as private or commercial considerations. Therefore, only they possess the statutory requirements and institutional capacity needed to adequately protect rights and uphold the rule of law in the context of criminal proceedings.[12]

Ensuring effective judicial oversight of cross-border data requests becomes especially important when such measures originate from a wide range of authorities operating within different criminal justice systems, with different criminal justice traditions. In fact, procedures to lawfully request, disclose and transfer the data sought (both within the EU and across the Atlantic) vary greatly depending on the law and jurisdiction under which a request is issued and/or has to be executed. Existing judicial cooperation instruments ensure that foreign requests for data are executed in line with the material standards applicable in the executing jurisdiction.

Judge-to-judge cooperation is at the basis of the EU principle of mutual recognition in criminal matters. EU member states' judicial authorities have a duty to recognise and execute criminal justice decisions issued by another EU country, based on the assumption that such decisions adhere to EU fundamental rights and rule of law standards. However, this duty of mutual trust does not exonerate judicial authorities from their responsibility to prevent the issuing and execution of foreign criminal justice measures from translating into an unjustified infringement of fundamental rights protections (as enshrined in national constitutions and, for EU member states, in EU primary and secondary law).

Requests for data issued by investigating authorities and addressed directly to service providers across borders raise crucial challenges in terms of effective judicial control, as well as material limitations to investigative measures.[13] These challenges arise not only when investigative or prosecutorial measures originate from EU member states which are constitutionally captured, and where the rule of law is institutionally or systematically violated (such as in cases of the

[11] Carrera S., and Stefan, M. (2020), *Access to Data for Criminal Investigation Purposes in the EU*, CEPS Paper in Liberty and Security in Europe No. 2020-01, February 2020.

[12] Lenaerts, K. (2017), "La Vie Après L'Avis: Exploring the Principle of Mutual Recognition (Yet Not Blind) Trust", Common Market Law Review, 54, p, p. 809.

[13] Brodowski, D. (2020), "European Criminal Justice – From Mutual Recognition to Coherence", in Carrera, S. Curtin, D., Geddes, A. (Eds.), 20 Year Anniversary of the Tampere Programme: Europeanisation Dynamics of the EU Area of Freedom, Security and Justice European University Institute, 2020, p. 230.

rule of law backsliding in Poland or Hungary), but for *any* government, including those which still qualify as 'liberal'.

And even in the scope of cooperation with third countries, the Court of Justice of the European Union (CJEU) has repeatedly highlighted the crucial importance of effective judicial protection and independent oversight to ensure compliance with EU legal standards.

In the recent *Schrems II* ruling, the Luxembourg Court has stressed that EU data-protection standards on cross-border transfers of personal data to a third country cannot be compromised by any form of access (including for the purpose of national security) by public authorities of that third country.[14] The CJEU has, in particular, clarified that transfers to a third country of EU personal data which "might undergo, at the time of the transfer or thereafter, processing for the purposes of public security, defence and State security by the authorities of that third country cannot remove that transfer from the scope of the GDPR".[15]

The CJEU has also reminded that EU international cooperation instruments cannot fall short of providing data subjects with recourse to an oversight body capable of guaranteeing compliance with data protection standards equivalent to those required by EU law.[16] In the same decision, the Luxembourg Court has also restated that EU-competent supervisory authorities must suspend or prohibit a transfer of personal data to a third country – and most notably the US – where EU legal standards cannot be complied with in that country.

[14] See Court of Justice of the European Union Judgment in Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, of 16 July 2020.

[15] Ibid para.

[16] Ibid. para. 105

Between January and June 2020, CEPS and the Global Policy Institute (GPI) at Queen Mary University of London (QMUL) jointly set up and ran a Task Force to identify the exact ways in which electronic information can be requested, disclosed and exchanged across borders in full respect of the multilayered web of legally binding rule of law, criminal justice, privacy and human rights' standards applying to intra-EU and international cooperation.

The Task Force provided a closed-door platform for debate among a selected group of EU and national policymakers, providers of internet and telecommunication services, prosecutors, lawyers, civil society actors, and academic experts. Interdisciplinary expert dialogue was promoted throughout the Task Force meetings, focusing on questions surrounding:

- principles and norms governing intra-EU and international judicial cooperation on cross-border data gathering.
- new instruments for private-public cooperation on cross-border data gathering being developed at the EU level, and also by third countries and at the international level, and their implications for the coherent application of EU criminal justice, privacy and data protection standards.
- specific issues linked to the different components of the e-evidence package, including legal basis, involvement of judicial authorities in the country of issuing and execution, notification duties, rights and responsibilities of private companies, and access to remedies.
- the Covid-19 impact on criminal justice cooperation within the EU, and initiatives related to the digitalisation of criminal justice, especially in the field of cross-border exchange of evidence in criminal matters.

This report builds upon previous CEPS and QMUL work on these topics.[17] It is divided into four parts, each reflecting key findings that emerged from the Task Force deliberations, as complemented by data collection and research by members of the CEPS Justice and Home Affairs Section. This data collection and research was conducted through a questionnaire and semi-structured interviews with EU prosecutors and judicial authorities from nine different member states,[18] as well as with European internet and cloud service providers and telecommunications companies, and US internet and cloud service providers.

Part I takes stock of the set of EU constitutional principles and legal instruments upholding the existing framework, initially for intra-EU judicial cooperation for data gathering in criminal matters (Section 1), and then for EU cooperation with third countries, most notably the US (Section 2). This part of the report assesses the extent to which the existing EU instruments and channels of internal and external criminal justice cooperation in the field of data gathering allow

[17] Carrera, S., and others (2015), *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to the Rule of Law and Fundamental Rights*, CEPS Paperback Series.

[18] AT, BU, HU, ES, IT, PT, RO, SE, SI.

investigating and prosecuting authorities to access and exchange electronic information across borders, while preventing conflicts of laws and jurisdictions.

Part II looks at initiatives promoted by third countries – and developed at the wider international level – to establish various forms of cross-border public-private cooperation for data gathering. Focus is given to the US initiatives under the CLOUD Act (Section 3), as well as to the ongoing cooperation under the Council of Europe Convention on Cybercrime (Section 4). This part of the report interrogates the compatibility of these US and international initiatives with EU criminal law and data protection *acquis* and looks at their potential implications for the consistent application of the EU system of fundamental rights and rule of law guarantees.

Part III examines the different (internal and external) components of the e-evidence package. It assesses the state of play in the inter-institutional negotiations of the e-evidence files, and raises concerns related to the legality, necessity and proportionality of the latter (Section 5). Factors of legal uncertainty that would arise from the introduction of the proposed e-evidence rules are also identified and considered (Section 6). The added value of the different proposals making up the e-evidence package is examined from the perspective of the different categories of stakeholders including, in particular, EU and US providers of internet, cloud and telecommunication services, as well as legal practitioners including judges, prosecutors and defence lawyers (Section 7).

Part IV draws conclusions that inform a set of recommendations for EU law and policymakers. Recommendations focus on possible normative, policy and operational solutions that, while supporting the objective of effectively investigating and prosecuting crime in the digital age, also preserve fundamental rights and trust in the EU Area of Freedom Security and Justice, as well as in transatlantic criminal justice cooperation.

PART I:
EU CONSTITUTIONAL, LEGAL AND OPERATIONAL FRAMEWORK OF INTRA-EU AND INTERNATIONAL JUDICIAL COOPERATION FOR CROSS-BORDER DATA GATHERING IN CRIMINAL PROCEEDINGS

1. INTRA-EU JUDICIAL COOPERATION FOR DATA GATHERING IN CRIMINAL MATTERS

1.1 Judicial cooperation and data gathering within the European criminal justice area

Cross-border access, collection and exchange of data in the fight against crime includes activities touching upon different but closely interlinked policy areas – namely those of law enforcement, criminal justice, privacy and data protection – which fall squarely under the remit of the European Union.

Each of these EU policy areas is upheld by a specific set of rule of law principles, and governed by a consolidated body of primary norms, which are dynamically interpreted by the CJEU. This body of principles and norms currently provides the constitutional framework of reference for the development of both intra-EU and international cooperation for the collection of electronic information in different phases of criminal proceedings.

The gathering of data sought in criminal proceedings affects different categories of fundamental rights – including not only the rights to privacy and data protection, but also fair-trial rights – that are judicially protected under EU law. One the one hand, under EU law, the rights of individuals whose data are held/processed for law enforcement of criminal justice purposes might only be limited under certain predefined legitimate circumstance, and in the presence of verified necessity and proportionality requirements. On the other hand, fair-trial rights are absolute rights which cannot be compromised for the sake of preventing, detecting, investigating and combating crime.

The Task Force members rightly noted that, under the EU legal system, respect for the rule of law does not only depend on effective law enforcement, but also on member states' compliance with the duty to effectively protect fundamental rights.

The involvement of the right oversight authorities in the different countries concerned by law enforcement or criminal justice access, collection, exchange and use of data represents a crucial rule of law requirement in the EU legal system. It also constitutes a condition essential to ensuring that EU privacy and criminal justice standards are effectively guaranteed throughout the Union, as well as in cooperation with third countries. Clear benchmarks have been developed by the CJEU about the level of independent oversight and judicial protection required throughout the issuing, validation and execution of such measures.

First of all, the CJEU has stressed that, in order to be legal under EU law, requests for data for combating crime need the prior validation of an independent administrative and/or judicial authority in the country of issue.[19] Over time, the CJEU has further developed the concept and

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

meaning of issuing authority in the context of criminal proceedings governed by certain EU judicial cooperation instruments (i.e. the European Arrest Warrant (EAW)). It has also specified the level of independence from the executive that judicial authorities (including prosecutors) must have in order for certain categories of criminal justice measure to be recognised and executed in another EU member state.[20]

Mutual-recognition proceedings may deal with cross-border data gathering (i.e. EIOs) and involve measures affecting inter alia the right to privacy and data protection. The CJEU is still due to clarify what level of judicial independence must be ensured by national authorities to effectively qualify as issuing authority in such proceedings. However, a longstanding European jurisprudence has progressively detailed the characteristics and levels of independent oversight that must be guaranteed over this type of activity. Data access must be subject to a prior review, carried out either by a court or an independent administrative authority, and "the decision of that court or body should be made following a reasoned request [...] submitted, *inter alia*, within the framework of procedures for the prevention, detection or prosecution of crime."[21]

The CJEU Advocate General (AG) Pitruzzella has recently set out important indications on who can issue requests for stored telecommunication data in the context of criminal investigations. In an opinion adopted on 21 January 2020, the AG reinstated the need for prior judicial review by an independent authority for every request, regardless of the type of data being sought.[22] The AG concluded that "the requirement that the access of the competent national authorities to retained data be subject to prior review by a court or an independent administrative authority is not met where national legislation provides that such review is to be carried out by the public prosecutor's office which is responsible for directing the pre-trial procedure, whilst also being likely to represent the public prosecution in judicial proceedings".[23]

The intervention of an independent judicial authority at the issuing stage of investigative measures entailing access to stored data is closely interlinked to the objective of ensuring a thorough ex ante scrutiny of the legality, necessity and proportionality of any interference with fundamental rights protected at the EU level. Where an effective protection of fundamental rights requires prior validation (judicial protection ex ante), the validating authority should not only be independent from the executive (the Minister of Justice) as required by the Court of Justice in its case law on the EAW, but also independent from the authority in charge of investigation and prosecution (i.e. the public prosecutor's office). Only the latter understanding will ensure an effective protection of the data subject's fundamental rights. This view has been

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

[21] Joined Cases C-203/15 *Tele2 Sverige AB v Post-och telestyrelsen* and C-698/15 *Secretary of State for the Home Department v Tom Watson & Others*.

[22] Opinion of Advocate General Pitruzzella, Case C-746/18, *H.K. v. Prokuratuur* (Request for a preliminary ruling from the Riigikohus (Supreme Court, Estonia)).

[23] Ibid. V (2).

confirmed most recently by AG Sanchez-Bordona in his opinion on the concept of judicial authority in the EIO Directive.[24]

Another key characteristic of the EU *acquis* on judicial cooperation for data gathering is the systematic ex ante involvement of competent judicial authorities in the member state of execution. Within the EU criminal justice area, the enforcement of cross-border investigative measures issued in the context of criminal proceedings is allowed by a system of mutual recognition of judicial decisions. Mutual recognition in criminal matters is strictly based on direct cooperation between member states' judicial actors. EU countries' judicial authorities are in fact required to mutually recognise and enforce each other's criminal justice measures based on the principle of mutual trust (i.e. the assumption that all member states comply with EU fundamental rights and rule of law standards).

As the CJEU has repeatedly clarified, the obligation to recognise and enforce another member state's criminal justice measure is not absolute, but rather it is subject to prior verifications and exceptions. In particular, the judicial authorities of the EU country of (requested) execution are responsible for preventing the enforcement of a foreign measure in their own jurisdiction from translating into unjustified abuses of fundamental rights (or at least their core essence) protected at EU and national constitutional level.[25]

Direct judicial cooperation and mutual 'peer review' of criminal justice decisions therefore represent the essential conditions for ensuring a trust-based functioning of an EU criminal justice area based on the rule of law.

The judicial authorities of the executing member states therefore remain in charge of the legal assessment, recognition and validation of any order received from other member states before referring the measure to a service provider for execution. In the EU legal system, service providers, which are private companies, have neither the legitimacy nor competency to make such an assessment, which is and should remain the prerogative of the state and its judicial authorities.

Ensuring that judicial authorities in the executing member state verify the impact that other EU countries' criminal justice measures might have on individuals' rights and freedoms constitutes a crucial legal certainty factor. In fact, the correct application of the so-called EU procedural rights *acquis*, as well as the delivery of remedies in cross-border criminal proceedings, relies upon the judicial control and intervention of competent authorities in both the issuing and executing countries.

The systematic ex ante involvement of independent judicial authorities in the country of execution of a cross-border data request becomes especially important in a context where different EU countries are affected by rule of law backsliding processes. Courts in several member states (including Germany, Ireland, Spain and the Netherlands) have increasingly challenged the assumption that criminal justice measures issued by other EU countries should,

[24] Opinion of Advocate Sanchez-Bordona, Case C-584/19, *Staatsanwaltschaft Wien*.

[25] Joined Cases C-404/15 and C-659/15 PPU *Aranyosi and Căldăraru*, 5 April 2016.

by default, be considered compliant with fundamental rights and rule of law standards enshrined in national constitutions or EU primary law.

Most recently, a court in Amsterdam stated that the Netherlands will stop extraditing suspects or convicts to Poland over concerns that the country's courts are no longer independent.[26] This decision came after the Karlsruhe Higher Regional Court (*Oberlandesgericht Karlsruhe*) ruling on the EAW,[27] in which the German court refused to surrender a suspect to Poland based on the lack of general or specific assurances that judges are independent from the executive. To a large extent, processes of 'constitutional capture' which inter alia undermine the independence of certain member states' judiciaries, have been more problematic since the outbreak of the Covid-19 crisis.

The issue of trust in cross-border cooperation for data gathering in criminal proceedings emerged as a central one in the Task Force discussions. Several Task Force members – including private sector representatives, defence lawyers and criminal law scholars from different EU member states – stressed that high numbers of direct cross-border requests do not automatically justify giving up legality checks in the executing state. This is especially, but not exclusively, because of different EU countries' sensitivities about possible foreign 'state interferences' and tensions with basic fundamental rights and criminal justice safeguards.

If reciprocal independent judicial oversight over data-gathering measures must be upheld in judicial cooperation between EU countries adhering to the principles and standards in the EU Area of Freedom Security and Justice, a higher level of scrutiny should by extension apply to cooperation with third countries such as the US and the UK. That is because, to these countries, the principle of mutual (but not blind) trust upholding EU cooperation in criminal matters does not apply.[28]

1.2 Legal instruments and tools for intra-EU cooperation

1.2.1 The European Investigation Order

The European Investigation Order (EIO) allows participating member states to issue and execute cross-border data-gathering measures based on the principle of mutual recognition of judicial decision in criminal matters.

The EIO establishes a framework for direct judge-to-judge cooperation based on mutual (but rebuttable) trust and clear division of labour between judicial authorities that, in the issuing and executing country, are respectively competent and responsible for the adoption,

[26] In July, the same court had already asked the CJEU whether the extradition of Polish suspects must be halted considering that "the independence of Polish courts and thus the right to a fair trial have come under increasing pressure."

[27] Ausl 301 AR 156/19.

[28] Carrera, S., Mitsilegas, V., Stefan, M. Giuffrida, F. (2018), *The Future of EU-UK Criminal Justice and Police Cooperation, Towards a Principled and Trust-Based Partnership*, CEPS Task Force Report.

validation, recognition and enforcement of investigative measures targeting different categories of data.

The EIO allows investigating authorities to order the collection of evidence (also in digital form) abroad. The authorities that are competent and responsible for issuing and/or validating requests for data sought in the context of a criminal case vary significantly between member states and are identified by national criminal procedural law provisions. By requiring EIOs to be issued or validated by a judge, an investigating judge or a public prosecutor competent in the case concerned,[29] the EIO Directive judicialises the issuing of investigative measures that involve the preservation and/or production of stored electronic information.

Judicial authorities of EU countries participating in the EIO legislation can currently use a standardised form to order the cross-border preservation and production (also simultaneously, and potentially in combination with other investigative measures) of different categories of information held by service providers in another member state, including content, traffic, and subscriber information. EIOs that mandate the preservation or production of certain categories of non-content data cannot lead to non-recognition or non-execution decisions based on the objection that such measures are not available in the state of execution. These include, most notably, EIOs targeting data that enables the identification of persons holding a subscription to a specified phone number or IP address.

The EIO allows judicial authorities to order the gathering of data across borders within a short deadline when this is required by the seriousness of the offence or in other particularly urgent circumstances. The EIO Directive also sets out the possible need for the execution, whenever practicable, of provisional measures such as the preservation of data within a 24-hour deadline.[30]

Assuming that the investigative measures included in the EIO do not contravene fundamental safeguards provided under their own legal system, nor undermine fundamental rights protected under EU law, the authority in the country of execution has the obligation to enforce the other country's EIO. The execution of an EIO takes place in the same way, 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.[31] One Task Force member noted that this way of working preserves specific material standards that users may trust, for example, if they store data, on purpose, in data centres in a particular member state (so as to avoid potential misuse of the criminal justice system in another member state, to their detriment). For example, some German lawyers choose to store certain data in Belgium as this country offers higher levels of protection in terms of client-attorney protection.

From the perspective of the investigation and/or prosecution, it was noted how authorities in the issuing state are often not the 'best placed' to perform investigative measures involving access to data held by service providers across borders. Interviews with prosecutors indicated

[29] Article 2 (c) (ii) of the EIO Directive.

[30] Article 32(2) of the EIO Directive.

[31] Article 9(1) of the EIO Directive.

for instance that unilateral action is not suited to investigate crime the digital evidence of which can only be collected through the execution of several data gathering measures addressed to various service providers in multiple jurisdictions. Direct coordination and cooperation among judicial authorities in different Member States was referred as key to secure timely execution of such measures.[32]

From the perspective of the service providers holding the data sought, the involvement of the judicial authorities with competence for recognising and executing the measures in the country of the EIO's material enforcement ensures legal certainty. The addressee of the EIO can trust that the investigative measures have been adopted following the right procedures. Therefore they do not have to invest time and efforts in the verification of whether the measures have been issued or validated by a competent authority. The cross-border data-gathering measure contained in an EIO becomes a domestic one once it is recognised and/or validated by the competent judicial authorities in the country of execution. This domestication allows the activation of well-established, secure and trusted channels of cooperation and exchange of data between service providers and investigating and prosecuting authorities.

Execution is mandatory, and there is no risk of liabilities for service providers under the EIO scheme, since the order is enforced by virtue of a legally valid decision adopted by a designated body in the legal system of execution.

From the perspective of the suspect or accused person, and data subject more generally, the involvement of the competent judicial authority in the country of execution also provides for access to effective criminal justice remedies. Suspects and accused persons can appeal before the judicial authorities of the executing state if the production or preservation of data executed by virtue of an EIO has resulted in a breach of certain rights. The intervention of an independent judicial authority in the country of execution therefore constitutes a crucial condition for upholding the fair-trial principles laid down in the EU Charter of Fundamental Rights.

The EIO Implementation Report (originally due in May 2019) has not yet been produced. This report is, however, necessary to properly assess if the current instrument for intra-EU data gathering in criminal matters works successfully.

Lessons still need to be learned from the EIO implementation, and some legal and administrative shortcomings still appear to affect its correct functioning.[33] Nevertheless there is no evidence nor consensus among prosecutors and/or judicial authorities showing that new instruments of intra-EU criminal justice cooperation for the gathering of data in criminal

[32] Joint Investigation Teams (JITs) represent another channel through which EU judicial authorities and law enforcement authorities currently cooperate (as well as with third countries' authorities) in order to collect electronic information across borders, especially in complex cross-border criminal investigations. JITs agreements enable national authorities to perform investigative measures in one or more of the states involved. During the interviews, several judicial authorities referred to JITs as a "flexible and informal way" to cooperate (also in real time) in the exchange of information and collection of data and evidence across borders. Eurojust provides increasing financial and logistical support to facilitate the formation and implementation of JITs, including in the area of cybercrime.

[33] Guerra, J.E., Janssens, C. (2018), "Legal and Practical Challenges in the Application of the European Investigation Order Summary of the Eurojust Meeting of 19–20 September 2018", Eucrim, 2019/1, pp. 46-52.

proceedings are urgently needed. On the contrary, research conducted during the Task Force implementation process has found clear examples of how efficient intra-EU judicial cooperation can be fostered through the EIO to secure timely access to, and collection of, different categories of electronic information held by private companies across borders.

All nine national prosecutors interviewed in the context of the Task Force research confirmed that cooperation for the cross-border gathering of data under the EIO is gradually improving, with national authorities becoming increasingly acquainted with both issuing and executing cross-border data-gathering measures through this mutual-recognition instrument. At the intra-EU level, the EIO is reportedly used for the collection of all types of data, including not only the content of electronic communications and metadata such as traffic data, but also basic subscriber information.

According to the interviewees, it is currently "very unusual" for issuing authorities to get a clear-cut refusal to recognise or execute an EIO. On the contrary, "dialogues among judicial authorities" often take place to identify the best way to execute the (potentially different) measures indicated in the order. EIOs including data-gathering orders are reportedly not only issued for the so-called 'list offences', but also for the execution of cross-border investigative measures related to less serious crimes. Even in such cases, EIO are normally executed except where the facts covered by the investigation do not constitute a criminal offence in the country of execution. A specific benefit of the EIO is that it allows judicial authorities to simultaneously require the cross-border execution of different investigative measures 'in one package'.

Cooperation under the EIO was described by the prosecutors interviewed as "working well", "swift enough" and suited to intra-EU cross-border data gathering "even in urgent cases". When cases are urgent, then real-time contacts, and cooperation between the judicial authorities in the member states of issuing and execution of an EIO, can be facilitated through Eurojust and the judicial authorities working at the National Desks of the countries concerned.[34] The European Judicial Network (EJN) contact points and liaison magistrates can also help speed up the transmission and exchange of EIOs. Several liaison prosecutors contacted for the Task Force research reported that – in particularly urgent circumstances – the issuing, transmission, and execution of data-gathering measures through an EIO can happen "in a matter of hours".

Several of the prosecutors also highlighted that direct contact among judicial authorities (including through national contact points at Eurojust) can help in preliminarily assessing the necessity and practical benefit of issuing an EIO containing a cross-border data-gathering measure. Examples have been reported of cases where, before an EIO is issued, liaison prosecutors working at Eurojust National Desks help their national authorities to verify important elements, through contact with the competent authorities in the country of envisaged execution, for instance, whether a certain I.P. address can be assigned to a user in the country of execution.

[34] In 2019, Eurojust supported judicial cooperation involving EIOs in 2,146 cases. See, Eurojust (2020), Eurojust Annual Report 2019 – Criminal Justice Across Borders, p. 6.

While the interviews did not reveal any major issues currently impacting the effectiveness of the EIO, some prosecutors pointed at challenges linked to the existing template of EIO forms. For example, the absence of a dedicated box to indicate the specific judicial authority competent for execution, and the limited number of suspects' names that can be included on the form. Other prosecutors referred instead to translation problems. For example, the poor quality of the translation leading to 'misunderstandings' in the country of execution, and lengthy translation processes resulting in cases where "an EIO is issued and validated in 30 minutes, but then translation takes a few days to be completed".

Lack of training and specialised human resources among member states' law enforcement and judicial authorities can also significantly affect the way in which requests for specific types of data are formulated. In turn, the unclear, imprecise or incomplete formulation of the data-gathering measures included under an EIO is likely to generate problems and reduce the chance of a swift validation (in the issuing country) and/or recognition (in the executing country). Delays in data production are also intrinsically linked to the complexity of technical processes and procedures that service providers have to implement in order to retrieve the data sought.

Several of the key challenges that currently hamper the effectiveness of EU cross-border data gathering appear therefore to be technical, practical and bureaucratic in nature, rather than related to ways in which judicial cooperation is designed under the EIO.

A key finding of the research is that the issuing of the EIO by judicial authorities is, in practice, often anticipated by cross-border preservation (or 'freezing') requests that police authorities send to their counterparts in another EU country, through the various networks of 24/7 Points of Contact (POC).[35] Such preservation or freezing requests are reportedly made in urgent cases, but also to prevent data being lost or erased by service providers at the expiry of the data retention period. In some countries these cross-border preservation requests are issued and executed by police authorities acting under the supervision of the competent national judicial authority (which vary depending on factors such as the crime investigated, or the stage of the criminal proceeding). In other jurisdictions, this type of cooperation happens purely at the police level and is not subject to judicial oversight. These different practices of police-to-police cooperation for the freezing of data therefore take place outside the existing EIO framework for judicial cooperation.

1.2.2 Digital platforms for transmission of requests and data

Effective judicial cross-border cooperation increasingly depends on judicial authorities in different jurisdictions transmitting and exchanging criminal justice decisions and transferring different categories of information (including data obtained from service providers), in a verified and trusted way.

Task Force members agreed that judicial cooperation needs infrastructures that allow judicial actors to issue and receive criminal justice decisions and transmit data through secure and

[35] There are currently several of these 27/7 police networks. In Europe, police authorities count on the one established under the Budapest Convention on Cybercrime, although similar networks include, for instance, Interpol's I-24/7 system, and the G8 countries' 24/7 network.

authenticated communication platforms. Such platforms should feature data protection standards capable of ensuring chain of custody (including the involvement of the right oversight authorities throughout the different phases of the communication and information exchange process).

The development of new technological solutions for exchanging information electronically represents concrete deliverables against the 'digital-by-default' principle entrenched in the EU member states Ministerial Declaration on eGovernment of October 2017. The need to upgrade and modernise judicial cooperation through information exchange in criminal cases across the EU has been expressly acknowledged by the European Council in its Conclusions of October 2018.[36] Most recently, the importance of equipping "judges, prosecutors, and legal practitioners with the tools to enable secure, swift and efficient cross-border communication with full respect of the highest standard of data protection" has been restated publicly by the Commissioner for Consumers and Justice in January 2020.[37]

The Task Force discussions focused especially on the current role and potential of digital communication tools and information exchange platforms available to judicial authorities. Specifically, to: a) request and obtain data held by service providers; and b) to exchange criminal justice measures and electronic information to be used as evidence among judicial authorities across the EU.

Currently, official platforms for transmitting data requests and transferring electronic information held by private companies have only been established by single EU member states at the domestic level. Countries including Austria, France, and Spain, for instance, have digital communication platforms in place that allow national investigating and prosecuting authorities to transmit data requests to private companies under their jurisdictions. Representatives of service providers operating in these three EU member states stressed that the existing systems work well.

Providers of telecommunication services contacted for the Task Force research in particular indicated that "if requests are transmitted via these platforms and following the agreed formats, then the process is very much automatised and the request is deemed admissible and valid". These systems are designed to secure a "high degree of formalisation" in respect of both the transmission of requests by investigating and prosecuting authorities, and the provision of answers by companies. In particular, the creation of Single Points of Contact (SPOC) on both sides proved useful at eliminating ambiguities in the communication process and reducing the time needed to process requests. Some telecommunication service providers are reportedly implementing the standards developed by the European Telecommunications Standards Institute, (ETSI) for a handover interface with their respective national authorities.

Some Task Force members observed that, while such national systems/platforms can serve as a model or 'blueprint' for transmitting domestic requests directed towards

[36] European Council meeting (18 October 2018), EUCO 13/18, https://www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf.

[37] See Council of the European Union (2020), Report on the outcome of the "Digital Cross-Border Cooperation in Criminal Justice" Conference, Brussels 21-22 of January 2020, p. 20.

telecommunications providers, replicating this for other kinds of service providers (e.g. internet and cloud service providers) may prove difficult. It was claimed that the variety of data requested from the latter is too diverse to be handled via a predefined system.

In any case, solutions developed at the national level to facilitate and streamline data exchange – between authorities and service providers under their jurisdiction – should be clearly distinguished from the portals some US internet service providers (ISPs) have created to receive requests directly from foreign authorities.

The information exchange platforms put in place in countries such as Austria, France, and Spain are strictly limited to domestic cooperation. Unlike US service providers (which can respond on a voluntary basis to foreign requests for non-content data), European telecoms operators and ISPs cannot transfer personal or telecommunication data directly to foreign authorities. The latter, in fact, need to channel their requests through existing instruments of international judicial cooperation (the EIO) and assistance (MLAs).

Data requests coming from foreign jurisdictions still need to be received and validated by the competent oversight authority in the country of execution. Only then can requests be transmitted to the relevant service provider under their jurisdiction, through the communication channels provided by the national platform for information exchange.

Members of the Task Force noted that the direct interconnection of service providers with foreign authorities following different constitutional and criminal law traditions is likely to generate new and largely unexplored challenges.

On the other hand, Task Force members restated the importance of establishing a single EU portal of communication and transmission of EIOs between competent judicial authorities. This view was also shared by different prosecutors interviewed. On several occasions, they identified the absence of an EU-level platform for digitally transmitting and exchanging information and documents (including not only data obtained from private companies under an investigative measure, but also judicial orders, court decisions, translations etc.) as one of the main practical challenges affecting cross-border judicial cooperation. Currently, EIOs are transmitted through traditional mail, courier, email or fax. Similarly, data obtained in the context of criminal investigations are copied onto storage devices (e.g. USB keys or CD-ROMs) and sent via traditional mail or courier.

As foreseen in the EU Council Conclusions of June 2016 on improving criminal justice in cyberspace, the e-Evidence Digital Exchange System (eEDES)[38] aims precisely to establish an EU-wide decentralised platform for communicating electronically, and exchanging evidence collected through the EIO and MLA instruments in a trusted, secure and admissible way.

The eEDES, in particular, aims to enable access to an interface allowing EU judicial authorities to complete EIO/MLA forms digitally, sign them electronically, send and receive them as a message, and attach documents to messages. The envisaged interface is designed only for communication and exchange of measures and data among EU judicial authorities. It does not

[38] The system was launched in December 2019 with a one-day event under the umbrella of the Expert Group on the e-Evidence Digital Exchange System.

cover transmission of information directly between national authorities and service providers across borders.

It has been agreed that the platform should be decentralised using the e-CODEX system as the tool for secure transmission of data. The e-CODEX is a decentralised IT system, connecting member states' national systems, which will enable requests and evidence to be exchanged securely between judicial authorities. The decentralised architecture of the system allows for information to be exchanged on a 'need-to-know' basis.[39] A key feature of the system, which is due to be operational by the end of 2020, is a complete repository of authorities competent to issue and execute EIOs. According to a high-level Commission official who took part in the Task Force debate, the system is neither very resource-demanding nor costly to implement. The Commission also stressed that it is now crucial to invest in training to enable the full potential of the future system.

Task Force members expect the eEDES to bring great added value to the existing framework for exchanging evidence across borders within the EU criminal justice area.

The need for improved 'digital justice' solutions has become even more evident since the Covid-19 crisis, which has significantly impacted the functioning of criminal justice systems across Europe and beyond. While the digitalisation of justice (and in particular 'remote justice solutions') is known to have a negative impact on defence rights (e.g. right to lawyer, access to case file, and presence at trial),[40] new infrastructure for digital communication among judicial authorities has the potential to make the current system of cross-border exchange of information in criminal proceedings more secure, direct, transparent and effective.

If properly designed and implemented, a digital platform for securely exchanging communication and information could not only speed up judicial cooperation in criminal matters, but also increase the personal safety of end users (i.e. judicial authorities).

Promoting digitalisation of judicial systems also constitutes one of the German Council presidency priorities. In a draft of EU Council conclusions presented and discussed at the meeting of JHA Councillors on Tuesday 1 September,[41] the German presidency invited the Commission to present a proposal to ensure the sustainability of eEDES, in particular by developing a governance and management structure that respects the independence of the judiciary and the constitutional requirements of the member states. In addition, the text asks the Commission to extend eEDES to other instruments of judicial cooperation in criminal matters, to support digitalisation of procedures relating to European arrest warrants.

The draft text also calls on the Commission to develop a comprehensive EU strategy towards digitalisation of justice and to further develop the monitoring of relevant digitalisation indicators in the EU Justice Scoreboard.

---

[39] EVIDENCE2E-CODEX (2020), *Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe. Conclusion report and feedback from the Joint WP4/EXEC,* Workshop on Merging Views Meeting technical and legal community to cross-fertilize views, Deliverable D4.3, p. 17.

[40] Fair Trials (2020), *Beyond the emergency of the COVID-19 pandemic: lessons for defence rights in Europe*, 20 July 2020. See also Fair Trials, COVID-10 Justice Project.

[41] Council of the European Union (2020), Draft Council Conclusions "Access to Justice – Seizing the Opportunities of Digitalisation" – Revised version, ST 10558 2020 REV 1.

2. EU LEGAL FRAMEWORK OF INTERNATIONAL JUDICIAL COOPERATION FOR DATA GATHERING

2.1 Coherence between internal and external action, and the promotion of EU values on the international stage

Strengthening the internal *acquis* on EU criminal justice and establishing a comprehensive Union legal framework on privacy and data protection have important implications for the development of EU action and cooperation on the international stage.

The EU has acquired an ever more prominent role in a number of matters relating to the area of freedom, security and justice, including criminal justice and law enforcement cooperation, as well as cybercrime and data protection. This has led the EU to progressively develop various instruments of bilateral cooperation with strategic partners (including the US), as well as in the context of multilateral cooperation initiatives (including the Council of Europe).

At the same time, the EU has adopted common internal rules on judicial cooperation in criminal matters, developed minimum standards of procedural rights in criminal proceedings, and established a legal framework on data protection. These entail a duty for the EU to prevent external initiatives from affecting the coherent application of the Union's benchmarks in these areas.

In fact, and unlike within the EU, cooperation with third countries is not based on "shared values and fundamental principles, the harmonisation of laws and procedural guarantees, or mechanisms for cooperation and supervisions".[42] Therefore, in adopting agreements with third countries – and more specifically in developing international agreements on data sharing – the EU must include "further and more detailed rules on the protection of fundamental rights."[43]

Article 2 of the Treaty on the European Union (TEU) explicitly entrusts the EU with the positive responsibility to not only respect, but also to promote – through external action – its fundamental rights and rule of law standards abroad.

Over the years, the EU has equipped itself with a set of legal instruments which, while enabling international cooperation for cross-border gathering and transfer of data in criminal proceedings, are also directed at ensuring that the coherence and efficiency of EU criminal justice and data protection *acquis* are not compromised. A clear example in this respect is the

[42] Brouwer, E. (2017), *International Cooperation and the exchange of personal data*, in Carrera and Mitsilegas (2017), 'Constitutionalising the Security Union: Effectiveness, rule of law and rights in countering terrorism and crime', CEPS Paperback, p. 74.

[43] Ibid.

so-called EU-US Umbrella Agreement,[44] which was designed specifically to secure EU data-protection standards in transatlantic transfers of data relating to criminal offences.

The CJEU has repeatedly stated the importance of ensuring that the coherence and effectiveness of fundamental rights protected under EU law are not compromised by cooperation with third countries.

In particular, the '*Schrems* saga' confirms that, to be legally viable and 'court-proof', EU instruments of international cooperation enabling cross border transfers of data must provide for effective – substantive and procedural – safeguards. The effectiveness of these safeguards depends, in turn, on their ability to ensure that international transfers of data do not translate into an unjustified interference with the fundamental rights of persons whose personal data are, or could be, transferred from the EU to a third country, and most notably to the US.[45]

In the *Schrems I* Case,[46] the Court of Luxembourg put particular emphasis on Articles 7 and 8 of the EU Charter. While Article 7 carries forward the obligation to prevent an arbitrary interference with the right to privacy, Article 8 embraces a more concrete obligation for the processing of personal data, including a requirement for an "independent authority".

The effectiveness of these safeguards depends, in turn, on the fitness of an international cooperation instrument to ensure that international transfers of data do not translate into unjustified interference with the fundamental rights of persons whose personal data are, or could be, transferred from the EU to a third country. Therefore, under EU law, a legal basis for cross-border transfer of data can only be valid if it guarantees individuals the effective possibility to access meaningful remedies for violations of rights, as protected under EU law. This is the express EU primary law requirement set out in Article 47 of the EU Charter of Fundamental Rights.

As the CJEU determined in its most recent *Schrems II* decision,[47] the consistent application of EU data protection law – as provided under the GDPR, read in light of the EU Charter of Fundamental Rights – cannot be compromised by a third country's laws and practices on data processing for public security purposes. On 16 July 2020, the CJEU yet again found that US internal security interests – and related digital surveillance practices – took precedence over any data-protection considerations. The recently concluded *Schrems II* case consequently led the CJEU to invalidate the Commission's decision on the adequacy of protection provided by the EU-US Privacy Shield.

The CJEU based its decision on the data protection risks deriving from data transfers from the EU to the US under the Privacy Shield which, the Court found, did not prevent US government

[44] The Umbrella Agreement "in and of itself shall not be the legal basis for any transfer of personal information", but rather represents an additional framework which aims to ensure that personal data exchanged between the EU and the US are protected in line with EU data protection requirements. The Agreement is currently under evaluation.

[45] Mitsilegas, V. (2015), "Judicial Concepts of Trust in Europe's Multi-Level Security Governance: From Melloni to Schrems via opinion 2/13", Eucrim, Issue 3/2015.

[46] Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650.

[47] Case *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, C-311/18, 16 July 2020.

authorities from performing mass surveillance activities which jeopardise the coherent application of EU fundamental rights guarantees. The CJEU found that the EU-US Privacy Shield's oversight mechanisms (such as the ombudsperson responsible for handling EU citizens' complaints) did not meet the legal benchmark of 'essential equivalence' with EU law data-protection standards, read in light of the EU Charter of Fundamental Rights. [48]

The finding that US law enforcement and internal security legislation takes primacy over data protection considerations, and fail to meet proportionality standards, as well as the verified lack of effective remedy in the US for EU data subjects (and the deficiencies in the Privacy Shield 'Ombudsman mechanism'), has led the CJEU to invalidate the latest EU mechanism for transatlantic transfers of data.[49]

In the *Schrems II* case, the Court of Luxembourg has stressed different key messages that are of central relevance for the Task Force discussions. The CJEU insisted on the importance of securing both effective and enforceable data subject rights (Article 8 of the Charter), and effective judicial remedies (Article 47 of the Charter).

The Court in particular made clear that in order for these rights to be effective and enforceable, individuals must be granted the possibility to access judicial remedies. In practice, this means that individuals must be granted access to a tribunal in order to seek judicial redress in case his or her data subject rights are violated.[50] Access to judicial remedies is therefore central to ensuring that the essence of fundamental rights (including most notably data subject rights) protected under EU law is effectively respected. The Court thus made it clear that the possibility to seek remedy before an independent judicial authority constitutes the essence of Article 47 of the Charter. This essential element cannot be limited[51] – not even when the data are transferred to a third country.

Against this backdrop, the need clearly emerges for EU instruments of international cooperation to include effective oversight mechanisms capable of verifying systematically – case by case – that EU fundamental rights standards are fully complied with by EU member states and third countries' authorities, and only limited to the extent that is strictly necessary and proportionate.

In *Petruhhin*, the CJEU has indeed submitted that, when a member state receives a request from a third state seeking the execution of a cross-border criminal justice measure (in the case at hand, the extradition of a national of another member state), that first member state must

[48] Rotenberg, M. (2020), "Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection", European Law Journal 2020, 1, p. 1-12.

[49] Kuner, C. (2020), *The Schrems II judgment of the Court of Justice and the future of data transfer regulation*, European Law Blog, 17 July 2020.

[50] See *Schrems* (Case C-362/14), op. cit., para 95.

[51] Lenaerts, K., 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal, 779–793.

verify that the execution of this measure will not prejudice the rights referred to in Article 19 of the Charter.[52]

This line of jurisprudence clearly shows that EU Member States judicial cooperation in criminal matters with third countries must be compatible with EU external benchmarks. It also highlights the importance to systematically involve EU national courts. The latter have a crucial role to play in ensuring that cooperation with third parties does not prejudice the coherent application of EU law, since they may ask for the intervention of the CJEU if the a third country request is believed to be in breach of EU fundamental rights, as enshrined in the Charter, should there be a connection with EU law in that case.[53]

2.2 Cooperation under the EU-US mutual legal assistance agreement vs transatlantic data gathering through direct private-public cooperation

As for the transatlantic framework of cooperation on criminal justice cooperation in gathering evidence, the standing EU legal basis for the collection and transfer of electronic information is the MLA Agreement with the US.[54] The Agreement complements existing bilateral treaties between the US and particular member states, and amends some of their provisions, if they provide for less effective avenues of cooperation.[55]

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 chance to effectively review the data-gathering measure issued by the other.

When channelled through transatlantic MLA agreements, US requests for data are subject to the judicial scrutiny of member states' competent authorities. Such scrutiny is designed to ensure that the rights of suspects and accused persons, as well as those of third parties and data subjects, are protected in line with EU and national criminal justice and data-protection standards.

Under the EU legal framework on judicial cooperation in criminal matters, service providers subject to the EU jurisdictions are not allowed to respond directly to US authorities' requests for data. Representatives of European providers of internet, cloud and telecommunication services which contributed to the Task Force research indicated that they never directly answer/execute foreign requests for data. Requests for data coming from foreign authorities are usually disregarded ("sent directly to the bin") or not directly executed. On receipt of cross-border requests, service providers reportedly tell requesting authorities to address/send the measure via the competent domestic authorities in the country of execution.

---

[52] 9 Case C-182/15, *Petruhhin*, Judgment of 6 September 2016, para. 60

[53] Ibid.

[54] 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.

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

From a perspective of individuals' rights, the involvement of EU judicial authorities in validating and executing US data requests channelled through transatlantic MLA agreements is especially important in light of the limitations that still affect the US Judicial Redress Act.[56] This piece of US legislation has been adopted to comply with the provisions of the EU-US Umbrella Agreement. Among other things, the Agreement requires the US to grant the right to access judicial remedies for data subjects whose data are transferred from the EU to the US in case the US authorities deny access or rectification, or unlawfully disclose their personal data. The Act currently only offers citizens of designated countries (including EU members states, minus Denmark) access to civil law procedures, not to redress actions in the field of criminal law.[57] Access to this type of procedures, however, does not qualify as an effective remedy under EU criminal law.

Derogations from the rule according to which transatlantic data transfer for law enforcement and criminal justice purpose must take place pursuant to the MLA process and related guarantees are possible, but only on exceptional grounds, as precisely enumerated and circumscribed by the GDPR.[58] In this regard, the European Data Protection Board (EDPB) has clearly 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".[59] The European Data Protection Supervisor (EDPS) has also recalled the importance of systematically involving EU member states' judicial authorities "as early as possible in the process of gathering electronic evidence" across the Atlantic.[60] Only with such involvement can EU authorities have the possibility to review the compliance of US orders with EU fundamental rights standards, and raise legitimate grounds for refusal where necessary.

If validated by the competent judicial authorities of the requested EU member state, incoming foreign requests (including those from the US) are to be executed as if they were domestic, by virtue of a compulsory order issued according to the procedures (and related safeguards) of the country of execution.

The same principle applies to EU authorities' requests for data channelled through MLA agreements and validated by competent US authorities.

To obtain data stored or held by companies falling under the US jurisdiction through an MLA procedure, requests originating from competent EU authorities must be: a) received, processed and validated by the US central authorities (i.e. the Office of International Affairs of the US

---

[56] In this regard see Bignami, F. (2015), *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, May 15, 2015, pp. 11-13.

[57] 28 C.F.R. §16.96(w)(3), (w)(9) (2012).

[58] See 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.

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

[60] 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, p. 3.

Department of Justice); and b) executed through a search warrant adopted by a US federal judge who has been satisfied of the existence of 'probable cause'. This is the US legal standard currently applying to any foreign law enforcement requests for access to content data by the Electronic Communications Privacy Act (ECPA), which protects wire, oral and electronic communications in transit. The same procedure also applies to foreign requests for data targeting US citizens or residents.

Contrary to the EU legal system, US law also envisages opportunities for direct private-public cooperation for cross-border preservation and production of non-content data sought in the context of criminal proceedings.

As far as requests originating from authorities investigating and prosecuting in EU member states, the Stored Communication Act (SCA) allows US companies to execute them – on a voluntary basis – as long as they target non-content data pertaining to non-US citizens or residents. Requests for non-content data are, in fact, currently received by the European subsidiaries of US internet or cloud service providers, which process them in line with their own internal guidelines.

US law furthermore allows US service providers to respond to foreign law enforcement authorities' 'emergency requests'. These direct cross-border requests are also assessed pursuant to the policies and standards set out by the addressed service providers, and irrespective of the 'probable cause' requirement. In urgent cases, EU member states' law enforcement authorities also simultaneously liaise with the US authorities who, in turn, facilitate the voluntary provision of the required material by service providers according to US law.

According to the Commission, this arrangement can work very well and, in exceptionally serious and urgent cases, data can be obtained within 24 hours.[61] Interviews with several US service providers confirmed that urgent requests are fulfilled if the requesting authorities effectively substantiate the existence of an emergency (including cases and situations linked to serious crimes such as kidnapping, murder threats, bomb threats and terrorism threats). Some US service providers even allow urgent requests to be addressed through 24/7 points of contacts, ensuring they are processed and executed outside of normal business hours if the emergency involves "the danger of death or physical injury to any person."

In this regard, it was reported that foreign authorities often fail to include the necessary information or specifications in their requests. In many cases, the requesting authorities fail to substantiate urgency. One US service provider reported that authorities often "consider urgent a request for data that they need for their work, but which is not essential to prevent an emergency involving the danger of death or physical injury to any person...". Refusal of requests

[61] 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), p. 84-85.

based on the lack of necessary information results in lost time for the company, and frustration for investigating and prosecuting authorities.

To avoid these types of situations, some US service providers have developed different sets of guidelines, that vary according to the type of data sought, to help non-US investigating and prosecuting authorities formulate and address their requests. One US service provider also created a dedicated 'law enforcement education programme' to help authorities across the EU formulate 'quality requests'. These requests should reportedly include at least: an indication of the legal basis upon which the data request is founded; the specification of the requesting authority, with evidence that it has the statutory power to issue the request; details about the crime object of the investigation; and why the information requested is necessary for the investigation. These elements are analysed by the receiving US service providers, which in some cases utilise teams of legal experts to assess whether incoming requests are legitimate and/or abusive.

One of the most challenging tasks that US service providers face when conducting assessments of direct requests (especially for requests 'with no precedents') is in verifying whether the authority issuing and/or validating requests for data is effectively entitled to do so, and for which crimes.

Even though voluntary cooperation and direct cross-border requests in urgent procedures can work in practice, issues such as conflict of laws remain largely unresolved. These issues are also likely to increase, given the current absence of an EU legal framework for direct (public-private) transatlantic cooperation on cross-border data access.

US service providers indicated that they reserve the right to seek clarification, and to challenge a foreign request in domestic court where it appears abusive or incomplete, or where it is inconsistent with relevant legal requirements under the jurisdiction of enforcement. This shows clearly how direct voluntary cooperation can generate legal uncertainty, resulting in loss of time and resources for the receiving company, and in frustration for investigating and prosecuting authorities.

Furthermore, it must be remembered that, from an EU criminal law perspective, this type of direct cross-border cooperation with service providers cannot be qualified as judicial cooperation in the field of data gathering. Rather, it represents a form of police/law enforcement investigative or crime-prevention activity.

For different EU countries, non-content data obtained through voluntary direct public-private cooperation channels does not qualify as evidence in criminal proceedings. Information gathered through such channels will clearly still be used by requesting EU authorities as a form of intelligence or 'investigative knowledge' in the context of a criminal investigation. Nevertheless, to have that same data admitted as evidence before a court, the issuing and execution of an MLA request becomes necessary.

The same principle applies to the admissibility of data (including content) obtained directly from US service providers through emergency requests. In such cases, the information is required to prevent or tackle imminent and serious threats to the life of individuals, to preserve the state security, or to secure critical infrastructure. The admissibility of such information as evidence before courts would, however, still require the issuing of an MLA request.

PART II:
THE US CLOUD ACT, DEVELOPMENTS UNDER THE BUDAPEST CONVENTION, IMPLICATIONS FOR EU LAW

3. THE CLOUD ACT

3.1 Solutions made in the US

US law enforcement and criminal justice authorities use a variety of domestic and international cooperation channels to seek and obtain cross-border data, from both US and foreign companies. The formal framework of judicial cooperation for data gathering at the transatlantic level is provided by the MLA Agreement with the EU. Nevertheless, the direct exercise of extraterritorial criminal jurisdiction for cross-border gathering of data held by service providers abroad has been a longstanding and – from an EU law perspective – highly problematic US law enforcement authority practice.[62]

As clearly demonstrated by the dispute underlying the case of *Microsoft Ireland v Department of Justice*, this type of direct cross-border criminal law enforcement has far reaching legal and jurisdictional implications when exercised over subjects, data and companies falling under the scope of EU criminal and data protection law.

Within the standing EU legal framework, service providers are in fact not allowed to respond to foreign authorities' direct requests for electronic information. They can only provide access to communication data sought for law enforcement or criminal justice purposes in cases "where a prior review has been carried out by a court or an independent administrative body", "following a reasoned request of [competent national] authorities submitted within the framework of procedures of prevention, detection or criminal prosecution." This requirement can, in principle, be waived but only in cases of "validly established urgency".[63]

In 2018, a new piece of US legislation – the 'Clarifying Lawful Overseas Use of Data Act', better known as the CLOUD Act[64] – was enacted. Its purpose was specifically to clarify that US law enforcement authorities are allowed, under their domestic legislation, to order US service providers to preserve or disclose "content of a wire or electronic communication and any record of other information" that is stored outside US territory.[65]

The CLOUD Act also calls for 'executive agreements' between the US government and foreign countries. These agreements are designed to allow the competent authorities of one country to directly order the production, preservation and wiretapping of data held or controlled by service providers that are under the jurisdiction of the other country. The first CLOUD Act

[62] Carrera, S. et al. (2015), op. cit.

[63] CJEU joint cases C-293/12 and C-594/12, Digital Rights Ireland Ltd, ECLI:EU:C:2014:238 – par (62).

[64] CLOUD Act, S. 2383, H.R. 4943.

[65] Section 103 of the CLOUD Act.

Executive Agreement was signed between the US and the UK in October 2019. It entered into force in July 2020.[66]

The CLOUD Act has recently been referred to as a "transmission belt for the American vision of governance in cyberspace",[67] and as an instrument which – in different respects – should facilitate the implementation of the so-called America First strategy.[68]

On the one hand, the CLOUD Act (Part I) reaffirms the power of US law enforcement to issue warrants mandating production, preservation and wiretapping of data, and to address them directly to US companies operating abroad. By doing so, it gives US authorities a 'legal shortcut' allowing the unilateral application of US laws over issues (cross-border access to data for law enforcement and criminal justice purposes), which have far-reaching transjurisdictional implications.[69]

However, the Task Force discussions highlighted how unilateral US initiatives promoting direct transatlantic cooperation between law enforcement authorities and the private sector create legitimate concerns for EU countries, as well as for companies and individuals subject to EU data protection and criminal justice standards. Such concerns become especially legitimate in times when the adequacy of US data-processing practices and privacy standards (most notably in the field of law enforcement and internal security) is constantly being disproved by the CJEU.

On the other hand, the CLOUD Act (Part II) promotes the conclusion of bilateral agreements which, while allowing foreign authorities to obtain different categories of data pertaining to their citizens or third-country nationals (including of the EU) directly from US service providers, reserve a higher level of constitutional protection and judicial scrutiny for foreign requests targeting US citizens and residents. At the same time, the CLOUD Act executive agreements are also designed to expand US authorities' power to access cross-border data directly from foreign service providers under the jurisdiction of the other signatory party.

3.1.1 Part I of the CLOUD Act

Part I of the CLOUD Act clarifies that US law enforcement actors have the authority to directly order the transfer of data from US companies abroad.

However, the type of extraterritorial enforcement of criminal jurisdiction, which is foreseen under US federal law, particularly by the Stored Communication Act (SCA),[70] does not automatically legitimise the transfer of such data from a foreign jurisdiction – and most notably from the EU – to the US. The execution of warrants issued based on the SCA, and mandating a

[66] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington, 3 October 2019.

[67] Rojszczak, M. (2020), "CLOUD act agreements from an EU perspective", Computer Law & Security Review, Volume 38, September 2020, p. 13.

[68] The White House (2017), 'National Security Strategy of the United States of America'.

[69] Abraha H.H. (2019), "How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis", 9 International Data Privacy Law 207, p. 213.

[70] 18 U.S.C. §2713.

cross-border transfer of data to US authorities, risks violating national provisions in the other country. Such risk has, in fact, led to litigation between recipients of such warrants and the US government, as clearly exemplified by Microsoft's decision to challenge a SCA warrant in December 2013. This well-known case directly caused the US legislative initiative that finally led to the adoption of the CLOUD Act, which became effective in March 2018.

Part I CLOUD Act amended the SCA with the intention of removing interpretative doubts about the extraterritorial effect of warrants issued by US authorities. It does so by indicating that the entity in possession, custody or control of data is required to provide it, regardless of whether this information is stored in the US or abroad.

At the same time, the scope of obliged entities has remained unchanged. This means that US providers of internet and cloud services subject to US jurisdiction might still be compelled – through orders issued unilaterally by US authorities – to produce, preserve or wiretap data in their possession, custody or control, when it (regardless of its location) is needed for ongoing US criminal proceedings.

And yet, from the perspective of US companies operating within the EU legal system, and therefore subject to the EU data protection and criminal justice framework, Part I of the CLOUD Act is still a cause of concern and legal uncertainty. Indeed, the Task Force discussions highlighted how, for US companies providing services in the EU, receiving a US law enforcement cross-border data-gathering measure will still bring the risk of being exposed to conflicts with the GDPR.

The GDPR provisions related to transfers of EU personal data to third countries (Chapter V of the GDPR) have been subject to many different readings and interpretations.[71] As a general rule, the GDPR establishes that a third country's measure mandating the transfer or disclosure of EU personal data should only be recognised or enforced if based on an international agreement (and most notably an MLA Agreement).[72] At the same time, the GDPR also foresees a number of derogations from this general rule. Outside MLA transfers, or "in the absence of an adequacy decision",[73] the GDPR also envisages that a transfer may be carried out only if it is "necessary for important reasons of public interest",[74] as recognised in EU law or in the law of the member state to which the controller is subject.[75]

Besides noting that transfers operated under such 'derogations' clauses are not, in principle, covered by the safeguards provided under the Umbrella Agreement, Task Force members also doubted that the public interest of a third country can constitute a sufficient condition for data transfer, in line with the GDPR requirements.[76] In particular, the EDPB and EDPS doubted the

[71] See, for Instance, Swire, P. (2019), *When does the GDPR Act as a Blocking Statute? The relevance of a Lawful Basis for Transfer*, Cross-Border Data Forum, November 2019.

[72] Article 48 of the GDPR.

[73] Article 49 of the GDPR.

[74] Article 49(1)(d) of the GDPR.

[75] See Article 29(7) of the GDPR.

[76] Annex to the EDPB-EDPS *Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection*, p. 6.

possibility of justifying data transfer to a third country (outside a MLA procedure) based solely on the 'compelling interest' of the data controller to execute a foreign authority's measure in order to avoid being subject to legal action in a non-EU state. The scope for lawful transfer of EU data to third countries – and in particular to the US – outside MLA procedures, has become even narrower after the invalidation of the Privacy Shield in July 2020. In fact, there is currently no EU adequacy decision ascertaining that the third country ensures an adequate level of protection to be interpreted in light of the *Schrems* principles.

Furthermore, in *Schrems II* the CJEU confirmed that the GDPR's provisions granting effective and enforceable rights to data subjects also apply when the data has already been transferred to a third country. The Court stressed that the essence of these rights would be prejudiced in cases where individuals are deprived of their right to seek judicial redress once their data have been transferred to third countries. The Privacy Shield has been invalidated precisely upon the Court's finding that in the US surveillance activities take precedence over privacy considerations, and that data subjects are not granted effective and enforceable data subjects right, nor effective and enforceable judicial remedies.

A US service provider that is also a member of the Task Force indicated how, in line with the EDPB and EDPS assessment of the CLOUD Act, "they reserve the right to challenge any CLOUD Act order or other law enforcement order that would be likely to expose them to a violation of the GDPR". This position certainly reflects a clear commitment to respect EU data protection standards, as well as to avoid the high financial penalties associated with breaches of GDPR provisions.

Even so, challenging a US data-gathering measure issued according to the CLOUD Act appears very difficult in practice. The CLOUD Act significantly restricts the circumstances under which an 'obliged entity' can actually file a motion to quash or modify the SCA warrant,[77] and only allows for an order to be modified or quashed if it is in 'the interests of justice'.[78] Such a formulation appears to clearly prioritise US authorities' investigative needs over the interests/rights of addressed service providers to challenge cross-border data-gathering measures.

Challenging a SCA warrant is even more difficult (if not practically impossible) for data subjects. In fact, while the CLOUD Act foresees limited possibilities for legal actions from the obliged entity (i.e. the addressed service providers), it does not envisage notification duties in relation to data subjects.

[77] Challenging a warrant is subject to two conditions, which need to be met jointly: a) the addressed service provider must have a reasonable suspicion that the person targeted is a non-US person that does not reside is the United States; and b) the service provider must verify the material risk of violation of third-country law.

[78] Cf. 18 U.S. Code §2703(h)(2)(B)(ii).

A European Parliament resolution[79] on the adequacy of the protection afforded by the EU-US Privacy Shield[80] had already highlighted in July 2018 that the Cloud Act enables US authorities to bypass existing EU safeguards guaranteed under the MLAT system. The resolution in particular recalled that "neither the Privacy Shield Principles nor the letters from the US administration provide clarifications and assurances demonstrating the existence of effective judicial redress rights for individuals in the EU in respect of use of their personal data by US authorities for law-enforcement and public-interest purposes".

Task Force discussions furthermore highlighted the significant imbalance that exists between, on the one hand, the wide-ranging data-gathering powers granted by the CLOUD Act to US authorities and, on the other hand, the limitations that US data privacy law imposes on the rights and possibilities of the defence in criminal proceedings. While the US prosecution can subpoena digital records from a service provider to build its case, US data privacy laws currently prevent the defence from requesting such information as potentially exculpatory evidence.[81]

3.1.2 Part II of the CLOUD Act

On several occasions, the US government has presented the CLOUD Act as made necessary by the constant increase of MLA requests. In particular, by the increasing numbers of requests originating from foreign law enforcement and criminal justice authorities and directed at obtaining data held by US companies.

As clearly stressed by a US government representative who took part in the Task Force debate, one of the key justifications is precisely that mutual legal assistance channels are no longer "sufficient to handle the flows of cross-border requests for electronic data" directed at providers of internet and cloud services with 'US citizenship'. In fact, to be executed, foreign MLA requests must first be received, scrutinised and validated by the competent US authorities, which assess the incoming requests for data against their own domestic criminal justice and privacy standards.

Judicial cooperation under MLA instruments certainly requires the deployment of adequate resources on both side of the Atlantic. This is particularly the case at the level of the US Department of Justice's Office for International Affairs (OIA), which acts as the central US authority and is responsible for receiving and scrutinising all incoming foreign requests against domestic US legal standards. Lack of sufficient financial and human resources – which are indeed crucial for the correct functioning of existing instruments of judicial cooperation – inevitably cause inefficiencies and delays.

---

[79] European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)).

[80] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176), C/2016/4176.

[81] See also, Wexler, R. (2019), "Privacy Asymmetries: Access to Data in Criminal Investigations", UCLA Law Review, Vol. 68, No. 1, 2021.

The same applies to the requesting authorities. Interviews conducted with several EU member states' prosecuting authorities have confirmed that MLA cooperation can work well if the necessary capacity and legal knowledge exist on the side of the country formulating the request. Improved technical and legal knowledge throughout the EU is needed to allow issuing authorities to formulate preservation and production requests that are up to US standards. Low-quality requests received by the OIA still have to be processed, and this causes delays.

If the investigating authorities in the country issuing an MLA request are experienced/well trained, they will include the right information. Furthermore, experience shows that simultaneously activating direct communication channels between competent authorities on both sides of the Atlantic can significantly help in processing requests and assessing their urgency. An example was given where, in particularly urgent cases, EU authorities forward an MLA request to the US while also telephoning the DOJ Office for International Affairs. Once the urgency is verified, a warrant can be obtained from a US judge "right away and the measure can be executed in a matter of a few hours".

Part II of the CLOUD Act calls for 'executive agreements' that would allow the competent authorities of both signatory parties to issue cross-border production and preservation orders targeting different categories of data – including the content of electronic communications – as well as wiretapping orders for the live interception of data. These would then be served directly to service providers under the jurisdiction of the other party.

Non-US investigating authorities currently face bureaucratic delays when seeking data held by US companies through the MLA process, as a result of the application of US domestic laws by competent US government and judicial authorities. The CLOUD Act's executive agreements have been presented as a legal solution to these delays.

These agreements, however, are also designed to significantly extend the extraterritorial outreach of US law enforcement authorities over non-US companies based in the territory of the other party. They do so in a non-reciprocal way (to the advantage of the US), introducing differential treatments and levels of safeguards based on criteria such as nationality or place of residence of targeted individuals (to the disadvantage of non-US citizens or residents).

3.1.3 The US-UK Executive Agreement

The asymmetrical and, from an EU law perspective, discriminatory nature of the CLOUD Act agreements emerges clearly from the analysis of the US-UK agreement on cross-border data access.[82] The US-UK agreement on cross-border data access constitutes the first CLOUD Act executive agreement to enter into force. It has repeatedly been referred to as the 'blueprint' for future agreements of the same kind.[83]

[82] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Oct. 3, 2019, U.K.-U.S., C.S. USA No. 6 (2019) (CP 178).

[83] See, for instance, Daskal, J., and Swire, P. (2019), *The UK-US CLOUD Act Agreement Is Finally Here, Containing New Safeguards, Just Security*. The US has now also signed a CLOUD Act agreement with Australia.

The UK-US agreement applies unequal targeting restrictions and minimisation provisions based on criteria such as nationality and place of residence. In terms of targeting restrictions, it permits US authorities to directly order preservation, production and wiretapping of data pertaining to UK citizens and third-country nationals (including EU citizens), as long as they are located outside the UK.[84] UK authorities are, however, prevented from using the agreement to directly target data of US citizens or US permanent residents.[85] UK data-gathering measures targeting US citizens or US permanent residents still need to be channelled through a traditional MLA process, and are subject to review by US governmental and judicial authorities.[86]

Therefore, 'US persons' – as identified in the text of the agreement – would still be granted the (higher) level of protection foreseen by US domestic legislation and traditionally applying to foreign authorities' requests for data processed through the MLA system. Such level of protection would instead not be granted to UK nationals, nor to third–country nationals (including EU citizens) whose data might be targeted by UK authorities using the agreement.

The nationality of individuals targeted by the measures envisaged under the agreement also determines the applicability of data-minimisation requirements. Strict requirements are imposed on UK authorities to minimise the acquisition, retention and dissemination of data pertaining to US persons.[87] Yet the same level of minimisation is not imposed for data requested by US authorities.

The Task Force discussions showed how these asymmetrical minimisation requirements are likely to result in significant additional legal hurdles and procedural duties for the authorities in the issuing country. When requesting data pertaining to non-US persons or residents, UK authorities will not only need to undertake the ordinary procedural steps and fulfil the domestic legal obligations that normally apply to the issuing of cross-border data requests. They will also have to perform new legally sensitive and technically complex tasks that, under the MLA system, fall instead under the competence and responsibility of the US central authorities and courts. Under the CLOUD Act agreement, however, those kind of legal process and verification duties are 'outsourced' to UK courts and authorities.

---

[84] US authorities' orders under the agreement are not authorised to target UK "governmental entities or authorities", "unincorporated associations with a substantial number of members located in the UK territory", and "corporations located in the UK territory", but they will be able to target UK nationals and third-country nationals. Regarding these last two categories of 'targets', the only limitation is the requirement that the targeted person is not "located in the UK territory". These targeting restrictions are without prejudice to the powers granted to US authorities under Part I of the CLOUD Act.

[85] Targeting provisions included in the agreement establish that, as long as the US is the 'Receiving Party' (i.e. the party towards which an order is directed), the UK is not allowed to seek data of : a) any governmental entity or authority thereof, including at the state, local, territorial or tribal level; b) a citizen or national thereof; c) a person lawfully admitted for permanent residence; d) an unincorporated association where a substantial number of members fall into categories b) or c); e) a corporation that is incorporated in the United States; or f) a person located in its territory.

[86] See, Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime.

[87] See US-UK Agreement Article 7(2-5).

In substance, it appears that CLOUD Act agreements are designed in a way that will significantly favour US authorities. On the one hand, US authorities will gain the power to obtain data pertaining to a wide range of US *and* third-country nationals directly from foreign service providers under UK jurisdiction. On the other hand, they will be no longer be responsible for performing important and sensitive legality checks and technical verifications over foreign authorities' measures when these do not target US persons.

Clearly, the agreement gives US and UK authorities the power to directly seek and obtain data that, while held by UK and US service providers, might still fall under EU jurisdiction, or pertain to a person entitled to legal protection under EU law. Operating outside EU legal channels for international data transfers, the CLOUD Act executive agreement threatens to undermine the coherent application of EU data protection and criminal justice *acquis*. The US-UK Agreement, in particular, falls short of meeting key requirements that, under EU law, must be complied with in intra-EU and international cooperation.

First, the US-UK Agreement does not expressly impose systematic *and prior* judicial authorisation for the issuing of investigative measures, which EU law would demand. The agreement generally indicates that cross-border preservation, production or wiretapping orders shall be subject "to review or oversight" by an "independent authority". It therefore leaves it to US and UK domestic laws to determine which are the authorities competent to review and authorise such measures. Such authorities, however, may vary depending on the categories of data sought, as well as the specific purpose for which data are requested. This is concerning, since it is envisaged that the cross-border data-gathering measures introduced by the agreement might also be used by "national security agencies",[88] which are traditionally subject to looser judicial oversight regimes. Another crucial shortcoming is the fact that such authorisation does not necessarily have to be granted prior to the order being enforced.[89]

Second, since data-gathering measures (including wiretapping) targeting individuals or data potentially protected under EU law are addressed directly to US or UK service providers, they are likely to be executed without the approval (or even the knowledge) of competent courts in the EU. The US-UK Agreement foresees a system of notification for affected third countries. However, such a mechanism is subject to broad exceptions,[90] and in any case cannot be considered to meet the effective oversight and judicial protection requirements that, under EU law, apply to transfers of data to third countries.

Different treatments based on nationality, low(er) levels of protection for EU citizens and data, and overall lack of transparency on how EU data will be processed, are not compatible with the EU Charter of Fundamental Rights, and conflict with EU secondary law on privacy, data protection and criminal justice. Transatlantic cooperation should instead be based on reciprocity and mutual respect of applicable laws and jurisdictional competences.

[88] Ibid., p. 2.

[89] US-UK Agreement Article 5(2).

[90] US-UK Agreement Article 5(10)

4. THE COUNCIL OF EUROPE FRAMEWORK: THE BUDAPEST CONVENTION AND NEGOTIATING ITS SECOND ADDITIONAL PROTOCOLS

4.1 A 'global playing field' for rule-making on cross-border data gathering, outside the EU legal framework

New rules on direct mandatory cross-border cooperation with service providers are also being discussed at the wider international level, in particular in the context of the forum provided by the Council of Europe Convention on Cybercrime (also known as known as the Budapest Convention).[91]

The Budapest Convention – which is open not only to members of the Council of Europe, but also other countries – currently includes more than 60 state parties. While the EU is not party to the Budapest Convention, this multilateral cooperation agreement has been signed by all EU member states.[92]

The Budapest Convention has been seen as an example of 'venue shopping' and rule-making in fields of law (i.e. cybercrime, police cooperation, criminal justice and data protection) where clear EU-level transnational rule of law standards exist.[93] In the past, 'serious concerns' have been expressed by representatives of EU institutions, with regard to some of the Budapest Convention provisions' compatibility with the EU data protection and criminal justice *acquis*.[94] Such concerns related, in particular, to the interpretation of the Convention's provisions enabling foreign authorities to access data held under another party's jurisdiction, outside EU and MLA channels of judicial cooperation.

Currently, a Second Additional Protocol to the Budapest Convention – which countries such as the US and the UK consider the new 'global forum' for rule-making on cybercrime issues – is being negotiated under the coordination of the Cybercrime Convention Committee (T-CY). The purpose is to agree international rules which, if adopted, would introduce instruments allowing new forms of unilateral and direct law enforcement access to data held by private sector actors under EU jurisdiction. The norms being developed under the envisaged Protocol cover policy areas (i.e. law enforcement access to data, cross-border gathering of evidence in criminal matters, and the protection of fundamental rights in such contexts) that are extensively covered by EU data protection and criminal justice *acquis*.

[91] Council of Europe Budapest Convention on Cybercrime (CETS N° 185), 23 November 2001.

[92] Although it has not yet been ratified by Ireland and Sweden.

[93] Carrera, S. et al. (2015), op. cit., pp. 64-65.

[94] Refer to http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN.

Member states' participation in negotiations of the Second Additional Protocol constitutes a risk for the coherent application of laws the EU adopted in the field of judicial cooperation in criminal matters (Article 82(1) TFEU) and data protection (16 TFEU). To prevent the adoption of international rules that affect common EU rules or alter their scope, the Commission has been appointed by the Council as the negotiator for the Second Additional Protocol.

4.2 The Budapest Convention

The Budapest Convention is a binding international treaty that equips law enforcement authorities of its state parties with several tools for preserving and collecting data sought at the domestic and cross-border level.

The Convention establishes a legal framework which requires states parties to introduce specific cybercrime offences (encompassing criminal activities and offences committed against, or by means of, electronic networks) in their national criminal law. It also sets minimum requirements on the criminal law enforcement powers and investigative instruments that state parties must make available to their national authorities. The latter are inter alia enabled to issue both preservation orders and production orders.

Preservation orders enable competent authorities of the state parties to secure the swift preservation of data, including traffic data, that has been stored via a computer system. These orders oblige any "person to preserve and maintain the integrity" of computer data (for a maximum period of 90 days – which can be renewed) when it is deemed necessary to enable "the competent authorities to seek its disclosure", where there are grounds to believe that the data are particularly prone to being modified or deleted.[95] The Convention furthermore requires its state parties to adopt "legislative or other measures" to ensure the "expeditious disclosure" to their competent authorities of "a sufficient amount of traffic data" to identify the service providers and the path through which the communication sought" (for preservation) was transmitted.[96]

The type of production orders currently envisaged under the Budapest Convention might be issued against both a person in the territory of the issuing party,[97] and against service providers providing their services in the territory of the issuing party.[98] Production orders addressed against a person might target different categories of data – as long as they are specified – which are in that person's possession or control, and which are "stored in a computer system or a computer-data storage medium". Production orders served upon service providers are instead limited to obtaining "subscriber information" in the possession or control of that service provider.[99]

[95] Budapest Convention Article 16.1.

[96] Budapest Convention Article 17.1.b.

[97] Budapest Convention Article 18.1.a

[98] Budapest Convention Article 18.1.a

[99] Budapest Convention Article 18.3.

The requirement that production orders can only be served to service providers offering services in the territory of the issuing party does not exclude the extraterritorial outreach and cross-jurisdictional implications of such measures. In fact, some countries interpret Article 18 of the Convention as allowing the issue of cross-border orders for the production of data which, although in possession or control of a service provider providing services in the issuing country, might still be stored abroad.

According to a senior US government official who took part in the Task Force debate, Part I of the CLOUD Act legislation has been introduced in the US precisely to implement the international obligations deriving from Article 18 of the Budapest Convention. Part I of the CLOUD Act, in fact, authorises US law enforcement authorities to warrant US companies to produce data stored abroad. At the same time, however, the data-gathering powers bestowed to US authorities under Part I of the CLOUD Act appear to be significantly wider than those envisaged under Article 18 of the Convention (not being limited to measures targeting subscriber information).

Article 18 is not the only provision of the Budapest Convention extending state party authorities' extraterritorial law enforcement and data-gathering outreach. The Convention expressly envisages the possibility for a state party to unilaterally request data across borders when this data is publicly-available,[100] but also when "stored computer data located in another party" is "accessed or received" by a state party through a computer system in its territory, based on the lawful and voluntary consent of whoever has lawful authority to disclose it.[101]

The Budapest Convention's provisions which – directly or indirectly – grant cross-border data-gathering powers to the authorities of the state parties, raise a number of legal and jurisdictional challenges from an EU data protection and criminal justice law perspective.

As already noted, EU law currently does not contain possibilities for direct cross-border cooperation between service providers subject to EU jurisdiction and law enforcement or criminal justice authorities from third countries. Doubts exist as to whether service providers in the EU can operate (intra-EU and international) cross-border data transfers simply based on the consent of the data controller. Under EU data protection law, the "data controller can normally only disclose data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required".[102] This view has also been recently reconfirmed by the EDPS.[103]

---

[100] Budapest Convention Article 32.a.

[101] Budapest Convention Article 32.b.

[102] Article 29 Working Party (2013), *Comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime*, 05 December 2013.

[103] EDPB (2019*), Contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention*), 13 November 2019.

Task Force members representing different categories of European internet and telecommunication service providers have clearly stressed that their national laws do not allow them to respond directly to foreign authorities' requests for data. These companies only answer requests from the competent authorities in the jurisdiction in which the end-user service is provided. Even in cases of cross-border investigations, they must always receive the requests via a national authority.

This position is consistent with the views expressed by the EU member states' judicial authorities interviewed. Specifically, they indicated that their national laws currently do not allow investigating and prosecuting authorities in their countries to *order* the production or preservation of data directly to service providers abroad. They recognised that some forms of direct private-public cooperation currently take place – but only on a voluntary basis – with US service providers, which under US law are allowed (but not obliged) to disclose non-content information to foreign authorities. None of the judicial authorities interviewed qualified this type of cooperation as a form of judicial cooperation in criminal matters. They were clear about the fact that, in their legal system, voluntary cross-border cooperation constitutes a form of law enforcement investigations.

EU member states' judicial and law enforcement authorities can and (currently do) make use of instruments and tools provided by the Budapest Convention. Yet EU law principles, rules, conditions and safeguards related to law enforcement and criminal justice access to data still apply. Member states' participation in international cooperation, such as that provided by the Budapest Convention, cannot compromise the coherent application of EU laws and policies on accessing data for criminal justice purposes. This means EU member states are entitled to use the data-gathering possibilities provided under the Convention, but only to the extent compatible with EU law.

It also means they are responsible for ensuring that third countries' interpretation and use of instruments provided under the Convention do not result in unlawful infringements of EU data protection and criminal justice rules.

The Budapest Convention does not itself define (or limit) the types of conditions and safeguards that apply to its provisions and the execution of the different investigative measures it establishes. It only provides that such conditions and safeguards shall be "appropriate in view of the nature of the power or procedure" envisaged.[104] In substance, the Budapest Convention leaves it to state parties to determine how to issue and execute measures requesting or mandating the preservation, disclosure and production of different categories of data. The exercise of law enforcement powers and procedures provided for by the Convention is therefore subject to the conditions and safeguards provided for under the domestic, international and supranational law applying to the different state parties.

[104] Budapest Convention Article 15(2).

Currently, the Budapest Convention on Cybercrime includes 65 state parties.[105] Out of these, 29 are non-members of the Council of Europe.[106] In a context where countries subject to different criminal law and data-protection frameworks are empowered to seek cross-border access to data for law enforcement purposes, the need emerges for clear definitions and agreements on the substantial and procedural guarantees applying to the issuing and execution of the data-gathering measures.

To date, however, parties to the Convention disagree on important legal and jurisdictional questions. Risks of conflicts of laws, for instance, are likely to arise due to the unclear definition that the Convention gives of 'subscriber information', which can be targeted through measures – such as the production orders – established by this Treaty.

In some state parties, the gathering of subscriber data does not need prior authorisation by an independent court and can be performed directly by the police or prosecutors. In other EU countries, the gathering of such data must be based on a court order (e.g. in the case of dynamic IP addresses, where there is the need to use traffic data to get subscriber data). Moreover, some state parties treat IP addresses as subscriber data. However, in the *Benedik v. Slovenia* case, the ECtHR has stated that additional safeguards are needed when analysing or storing traffic data – including dynamic IP addresses – in quantities that allow profiling of individuals. According to such interpretation, dynamic IP addresses cannot be equated to subscriber data since their production (upon execution of a law enforcement order) affects additional fundamental rights.

4.3 The Second Additional Protocol

The CoE Cybercrime Convection Committee (T-CY) is currently coordinating negotiations for a Second Additional Protocol to the Budapest Convention, the conclusion of which is foreseen by the end of 2020.[107] In this context, discussions on instruments allowing remote access by law enforcement authorities to servers and computers located in foreign jurisdictions (outside existing MLA agreements) have been ongoing.

The envisaged Second Additional Protocol aims to develop a new multilateral framework providing state parties with broader opportunities for unilateral cross-border data gathering.

In terms of objectives and scope, the negotiations centre on four main blocks identified in the Terms of Reference for the preparation of the Second Additional Protocol:[108]

---

[105] In addition to the 65 current parties to the Convention, a further nine countries have signed it and been invited to accede the Convention. A further 28 states "are believed to have legislation largely in line with this treaty and a further 52 to have drawn on it at least partially".

[106] The Budapest Convention has been signed by all EU member states but has not yet been ratified by Ireland and Sweden.

[107] The decision to undertake the preparation of a Second Additional Protocol to the Budapest Convention on Cybercrime was taken by the T-CY in June 2017. This decision was based on the recommendations of the T-CY Cloud Evidence working group from 2015 to mid-2017.

[108] See, https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b.

- provisions for more effective mutual legal assistance (such as expedited MLA procedures for subscriber information, international production orders, joint investigations, and emergency procedures).
- provisions on direct cooperation with service providers in other jurisdictions regarding requests for subscriber information, as well as preservation requests and emergency requests.
- clearer framework and safeguards, including data protection requirements, for existing practices on cross-border access to data.
- safeguards, including data protection requirements.

The preparation of the Additional Protocol falls under the responsibility of the T-CY, which is composed of representatives of the state parties to the Budapest Convention on Cybercrime.[109] A Protocol Drafting Group including seven representatives of state parties to the Budapest Convention (working in sub-groups) has been established to assist the T-CY Plenary in the preparation of the Additional Protocol.[110]

The norms developed in the context of the Second Additional Protocol to the Budapest Convention might have given rise to obligations conflicting with the EU – internal and external – legal framework dealing with cross-border access to data. To prevent this, the Council authorised the Commission to participate in negotiations on behalf of the EU and its member states.[111] The European Commission is in fact currently participating with 'ad hoc experts' in the meetings of the Protocol Drafting Group.

The negotiations are held in closed-door sessions. According to the Terms of Reference for the preparation of the Second Additional Protocol, the T-CY may hold public hearings, publish drafts of its work, and invite submission of public comments from external actors. These actors include civil society organisation, data protection organisations and industry. A provisional draft text of the Second Additional Protocol was made publicly available for that purpose in October 2019.[112]

The draft reflects how progress made in the negotiation process mostly relates to provisions dealing with "direct disclosure of subscriber information" (Section 4 of the Draft Additional Protocol), and with "giving effect to orders from another party for expedited production of data" (Section 5 of the Draft Additional Protocol).

Several members of the CEPS Task Force provided written comments focusing on the draft provisions included in these sections.[113] They expressed concerns about the draft provisions

[109] According to Terms of Reference, negotiations are due to take place during the day after the regular T-CY Plenary meetings.

[110] Between September 2017 and July 2019, the T-CY held four Drafting Plenaries, seven Drafting Group meetings, two subgroup and ad hoc Group meetings.

[111] Council of the European Union (2010), Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), COM(2019) 71 final, Brussels, 5 February 2019.

[112] See, https://rm.coe.int/provisional-text-of-provisions-2nd-protocol/168098c93c .

[113] See, https://www.coe.int/en/web/cybercrime/protocol-consultations.

included in Section 4, and the possibility they envisage to allow the competent authorities of parties to order the disclosure of "specified, stored subscriber information" under the possession or control of a service provider in the jurisdiction of another party. Several stakeholders who took part in the consultation process noted that legal certainty could only be achieved through involving – meaningfully and systematically – the competent authorities in the jurisdiction where the measures would be executed.

In their contribution to the public consultations' process, Task Force members stressed that direct private-public cooperation for cross-border data gathering cannot be considered "a satisfactory alternative to judicial cooperation" between competent authorities across borders. These mechanisms, in fact, undermine the "essential duties of national judicial authorities to ensure that the rights of its citizens are not infringed, compromised or undermined".[114]

Draft Article 4(5) foresees the possibility for a party to require that an order issued to a service provider in its territory is simultaneously notified to its authorities. The designated authority of the receiving party may instruct the service provider not to disclose the information if specific conditions or grounds for refusal apply (as provided by Articles 25.4 and 27.4 of the Budapest Convention). This is, however, not compulsory, but remains at the discretion of the parties, which have the option to either require notification by the requesting authority, or to foresee a duty for service providers, which receive a cross-border order to consult with the competent authorities in the receiving party. As noted by some Task Force members, "it is unclear why such an important additional safeguard that provides legal certainty for both the service provider and the affected user shall be left to the discretion of each party to be implemented."[115] Moreover, Article 4(5) does not specifically mention which type of authority in the requested state orders are to be notified to and possibly reviewed by.

Parties are left with a large amount of discretion to define who are the authorities competent to issue the envisaged cross-border orders. In this regard, Task Force members noted that both the "case law of the CJEU and the ECtHR clearly stipulate the requirement of a prior review of production orders in respect of stored user data by an independent authority".[116] However, not all state parties are subject to the same legal standards, and in some cases (e.g. under US law)[117] subscriber information can be obtained by a simple administrative measure, without any prior judicial oversight.

Lack of involvement of the authorities in the country of execution, and large discretion left in the definition of who is an issuing authority, become especially problematic in light of the very broad interpretation that the explanatory report to the draft provision gives to the term 'subscriber information', included in Article 18 (3) Budapest Convention. Such interpretation

---

[114] CCBE (2019), *Comments Draft 2nd Additional Protocol to the Convention on Cybercrime Provisional draft text of provisions (1 October 2019) on Language of requests, Emergency MLA, Video conferencing, direct disclosure of subscriber information, and giving effect to orders from another Party for expedited production of data*, 8 November 2019.

[115] EuroISPA (2019), *EuroISPA's comments on the provisional text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime*.

[116] Ibid.

[117] 18 U.S.C. § 2703(c).

includes IP addresses and subscriber information for an IP address. This reading would therefore significantly expand the cross-border data-gathering opportunities of state parties, but at the same time increase risks of conflicts of law. This would be especially true in cases where the envisaged orders are directed at service providers under the jurisdiction of countries where IP-address requests are subject to different (i.e. higher) standards to requests for basic subscriber information such as name, address and contact details.

Further criticism has been expressed by Task Force members with regard to the lack, in the published text of the draft Second Additional Protocol, of clear grounds of refusal for the absence of double criminality, or when the requested data are covered by professional secrecy/legal professional privilege. Nor are there guarantees capable of ensuring that production orders targeting subscriber information can only be issued for serious crimes.

Taken together, the remarks highlight the manifold potential antinomies that this new international agreement could generate, not only with EU criminal justice and data protection laws, but also with the legal framework established under other CoE instruments, and most notably the ECHR and the Convention 108+.[118]

To safeguard the application of EU law between EU member states against potentially diverging provisions in the Second Additional Protocol, the Commission has requested a "disconnection clause providing that the Member States shall, in their mutual relations, continue to apply the rules of the European Union rather than the Second Additional Protocol".[119] The Commission also stressed that the Second Additional Protocol may only apply "in the absence of other more specific international agreements binding the European Union or its Member States and other Parties to the Convention, or, where such international agreements exist, only to the extent that certain issues are not regulated by those agreements. Such more specific international agreements should thus take precedence over the Second Additional Protocol provided that they are consistent with the Convention's objectives and principles."[120]

These considerations have been explicitly included in the negotiation directives[121] annexed to the Council Decision authorising the Commission to participate, on behalf of the EU,[122] in negotiations on a Second Additional Protocol. Clearly, the aim of the envisaged clauses is to guarantee the integrity of the EU legal order, and to ensure that the consistent application of EU laws is not compromised by the Second Additional Protocol entering into force.

---

[118] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)

[119] European Commission (2019), Annex to the Recommendation for a Council Decision authorising the participation in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), Brussels, 5 February 2019.

[120] Ibid.

[121] In the Council's negotiating directive, the term 'disconnection clause' has been replaced with the term 'clause'.

[122] Council of the European Union (2019), Council decision authorising the European Commission to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), Brussels, 21 May 2019.

The final text of the Protocol is still being negotiated. However, it is undisputed that the envisaged provisions on cross-border production orders cover areas – including judicial cooperation in criminal matters, procedural rights, as well as data protection and privacy safeguards – where the EU has already set its own standards and adopted legislation.

Against this background, it is concerning that the Council of Europe Legal Service – when asked for its opinion about the legal implications of the inclusion of such a disconnection clause – noted that this type of provision could "have the potential to create unnecessary divisions between the parties and legal uncertainty about applicable standards". It also noted that "instead of disconnecting, the European Union and its member states should fully take advantage of the existence of a well-functioning multilateral instrument encompassing 63 state parties worldwide, including most important strategic partners".[123]

As noted in the same Option, however, this type of 'special clause' has already been included in the Amending Protocols to CoE Conventions. For instance, the Amending Protocol to the Data Protection Convention 108 uses a special clause in the context of cross-border data flows. Such special clauses enable parties to refuse the transfer of personal data if they are "bound by harmonised rules of protection shared by States belonging to a regional international organisation."[124]

[123] See, Legal Opinion on Budapest Cybercrime Convention, Use of a 'disconnection clause' in the second additional protocol to the Budapest Convention on Cybercrime, Strasbourg, 29 April 2019.

[124] See Article 17.1 of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which modifies Article 12 of the Convection 108 (new Article 14).

PART III:
THE E-EVIDENCE PROPOSAL

5. THE E-EVIDENCE PACKAGE

5.1 Origins and rationale

At the EU level, the first official call for new tools allowing unilateral cross-border access to electronic data held by service providers was made in 2015, when the European Commission presented the European Agenda on Security.[125]

Designed under the lead of the Commission's Directorate General for Migration and Home Affairs, the Agenda set forth the strategic framework for the EU's work on internal security over the 2015-2020 period. This strategic framework, which promoted various forms of co-option of the private sector in the fight against crime, also called for "a new approach to law enforcement in the digital age", and in particular for the establishment of "public-private partnerships to structure a common effort to fight online crime".[126]

At the root of the Commission's choice to develop a new normative regime for public-private cooperation on cross-border data gathering lies the claim that "judicial cooperation is often too slow for timely access to data and can entail a disproportionate expense of resources".[127]

In reality, an independent review of the information on which the Commission justified the need for these developments later revealed a lack of statistical data that clearly proves that direct cross-border cooperation with service providers is more effective or successful (in terms of measures executed) than traditional judicial cooperation instruments.[128]

The Commission also stressed that, for a number of EU member states' law enforcement authorities, direct cross-border cooperation with service providers (especially those based in non-EU countries, and most notably in the US) has increasingly become "an alternative channel to judicial cooperation".[129] The *Yahoo!*[130] and *Skype*[131] cases in Belgium were quoted by the

[125] 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.

[126] Ibid. p. 20.

[127] European Commission, Commission Staff Working Document 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, Brussels, 17.4.2018, hereafter 'the Impact Assessment', p. 9.

[128] González Fuster, G., and Vázquez Maymir, S. (2020*), Cross-border Access to E-Evidence: Framing the Evidence*, CEPS Paper in Liberty and Security, No. 2020-02, February 2020.

[129] Ibid.

[130] Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N of 1 December 2015.

[131] Hof van Cassatie of Belgium, SKYPE Communications Sarl, No. P.17.1229.N, 19 February 2019.

Commission as examples of cases where national courts dealt with the extra jurisdictional implications deriving from the use of domestic production orders over companies whose main location is outside the requesting country but which provide a service within its jurisdiction.

In the Commission's view, the justification for new EU-wide rules on mandatory public-private cross-border cooperation therefore derives from the need to provide an EU legal basis for unilateral initiatives adopted by some member states acting outside the EU legal framework. The reason for this is to speed up cross-border data gathering in criminal investigations by bypassing existing channels of judicial cooperation. The Commission, in fact, claimed that such channels simply cannot sustain the constantly increasing volume of cross-border law enforcement requests for data.

The e-evidence proposals were tabled not even a year after the expiry of the deadline for the implementation of the EU Directive establishing the European Investigation Order (EIO).

The Commission stated at the time of the e-evidence proposal's publication that the different procedures foreseen by the EIO Directive for cross-border production and preservation of data "would still be too long, and therefore ineffective".[132] This claim was made despite a lack of available official information related to the EIO's functioning and outcomes for the purpose of collecting digital information in criminal proceedings. Indeed, the claim has not been confirmed by the prosecutors and judicial authorities who contributed to the Task Force deliberations and research.

Some Task Force members observed that, to a large extent, the e-evidence rules proposed by the Commission were designed to solve a longstanding EU-US policy issue. Specifically, this concerned the challenges faced by members states' authorities in ensuring access to different categories of data held by US companies providing cloud and internet services in the EU.

To date, EU authorities' transatlantic judicial requests for data must be channelled through existing mutual legal assistance treaties (MLATs), and therefore validated and executed by the competent US authorities. The latter, however, are chronically understaffed and underfinanced, and are still not supported by specialised US judicial bodies working especially on foreign requests.[133] Currently, US law also allows service providers to directly respond – but only on a voluntary basis – to foreign requests originating from non-US authorities when they target non-content data pertaining to non-US citizens or residents.

If adopted, the Proposed Regulation on European Production and Preservation Orders would allow EU member states' authorities to directly order a wide range of foreign service providers – including, but not limited to, US providers of cloud and internet services – to preserve and produce different categories of data, including content.

The Task Force discussions highlighted how the introduction of an EU framework on direct public-private cooperation is intended to address the risk of 'legal fragmentation' linked to the multiplicity of national approaches to cross-border (and most notably, transatlantic) data

[132] Impact Assessment, p. 23.

[133] Carrera, S., Stefan M. (2020), op. cit., p. 19.

gathering. At the same time, it is intended to solve a financial issue (i.e. the need for countries to deploy adequate resources to deal with high numbers of incoming requests). It does so by outsourcing – from states to private companies – the responsibilities (and associated costs) related to the execution of cross-border data-gathering measures.

To address what is ultimately an issue of cross-border law enforcement outside existing EU and international judicial cooperation channels,[134] the Commission proposed the introduction of new criminal justice rules. The Task Force discussions have highlighted how the e-evidence proposal risks blurring the boundaries between different policy fields (law enforcement and criminal justice cooperation) which – under the EU system – are governed by a different set of principles and rules. The Task Force also helped clarify how the proposals would transfer to service providers a set of functions and responsibilities (i.e. those related to the execution of a foreign criminal justice measure) that, traditionally, are entrusted to judicial authorities. Throughout the Task Force deliberations, it furthermore emerged how – by enabling direct extraterritorial enforcement of EU member states' criminal jurisdiction on companies subject to the legal frameworks of third countries – the proposals would also create confusion between the EU internal and external action in the field of cross-border data gathering in criminal matters.

5.2 State of play

In April 2018, the Commission tabled two legislative proposals (one for a regulation,[135] and one for a directive[136]) on e-evidence.

These proposals are intended, in particular, to enable European Production Orders (EPOs) and European Preservation Orders (EPO-PRs), issued by one member state, to be addressed directly to service providers based in another member state, and without needing the systematic ex ante involvement of judicial authorities in the latter. The company or its legal representative would be responsible for receiving and executing the EPOs and EPO-PRs.

Different judicial authorities would be responsible for issuing the proposed orders, depending on the types of measure and data concerned.[137] Prior validation by a court would be needed for production orders targeting 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 by prosecutors as well, and

[134] Mitsilegas (2017), "The Security Union as a paradigm of preventive justice: Challenges for citizenship, fundamental rights and the rule of law", in S. Carrera and V. Mitsilegas (Eds.), Constitutionalising he Security Union: Effectiveness, rule of law and rights in countering crime and terrorism, CEPS Paperback, pp. 14-16.

[135] European Commission (2018), Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Strasbourg, 17.4.2018.

[136] European Commission (2018), 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, COM(2018) 226 final, Strasbourg, 17.4.2018

[137] Article 5 of the proposed regulation.

for all categories of crime. EPOs could be issued by prosecutors and judges for all types of crime, and regardless of the type of data concerned.

The Commission decided to qualify the measures proposed under the regulation (i.e. EPOs and EPO-PRs) as instruments of judicial cooperation in criminal matters. It therefore selected Article 82.1 of the TFEU as a legal basis for its proposals on the so-called e-evidence package.

The Commission's qualification of the new instruments as a form of judicial cooperation 'building upon' the existing model of mutual recognition in criminal matters proved highly controversial among EU member states and other EU law-making institutions.[138]

There are tested principles, rules and procedures governing EU judicial cooperation in criminal matters, which systematically require the involvement of judicial authorities in the country of execution to enforce a foreign criminal justice decision. In a letter addressed to Vera Jourova – then EU Commissioner for Justice – ministries of eight EU countries[139] stressed that such a choice of legal basis for the proposed EPO and EPO-PRs (which do not foresee the systematic ex ante involvement of judicial authorities in the country of execution) would bring about a radical departure from these principles, rules and procedures.

In November 2018, the Council of the European Union adopted its general approach on the draft regulation.[140] The general approach is deemed to reflect a position of political compromise among the 27 member states ahead of negotiations with other EU law-making institutions. The major amendment proposed by the Council, in comparison to the text elaborated by the Commission, is the introduction of a system of limited notifications to the authorities of the EU country where the orders are addressed to be executed.[141] Such a notification procedure was primarily intended to address concerns related to the lack of involvement of the authorities in the country of execution.

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, 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 within its own jurisdiction, it must inform the state of execution and give it an opportunity to flag whether the data may fall under: data protected by immunities and privileges; data subject to rules on determination and limitation of criminal liability related to freedom of expression/the press; or data whose disclosure may impact the fundamental interests of the state. The issuing authority shall take

[138] Stefan, M. and González Fuster (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 Research Paper No. 2018-07, November 2018 (updated in May 2019), pp. 30-35.

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

[140] 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.

[141] Ibid., Article 7a.

these circumstances into account as if provided for under its own national law,[142] and withdraw or adapt the order where necessary.

Over the course of 2019, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) produced an extensive set of working documents[143] highlighting critical aspects of the proposals, and raising doubts related to their suggested legal basis, as well as their necessity and proportionality. In November 2019, the European Parliament's rapporteur on the e-evidence file, Birgit Sippel, published a report on the draft regulation.[144]

Sippel's report presents fundamental differences from both the Commission's proposal and the Council's general approach. It proposes an enhanced level of independent judicial scrutiny for the adoption or validation of the orders in the issuing country. It also envisages the introduction of mandatory notifications to both the affected state (the EU country of residence of individuals covered by the production orders) and the state of execution. Contrary to the notification system proposed by the Council, those envisaged by the EP rapporteur would only allow for the execution of production orders by the addressed service provider when the notified member states do not raise grounds for refusal.

Unlike the Commission's proposal and the Council General approach, which distinguishes between four different categories of data (i.e. subscriber information, access data, traffic data, and content), Sippel's report sticks to the data categorisation already adopted in EU law and member states' law, which only encompass three categories of data (i.e. subscriber, traffic, and content).

The positions so far expressed by the different EU institutions therefore diverge substantially over several important elements of the proposed legislation (see Tables 1 and 2 below). These include, most notably, the level of judicial protection required at the issuing phase, the nature and quality of involvement of competent judicial authorities in the member states different from the issuing one, the level of data protection to be ensured depending on the type of information targeted by the proposed orders, and the exact ex ante and ex post procedural safeguards guaranteed to the different categories of companies and individuals potentially affected by the envisaged measures.

[142] Ibid., Recital (35c).

[143] European Parliament, Public Register of Documents.

[144] European Parliament (2019), Draft Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (COM(2018)0225 – C8-0155/2018 – 2018/0108(COD)) Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Birgit Sippel, 24 October 2019.

Table 1. Conditions for issuing and oversight

COM Proposal	Council GA	EP (Sippel Report)
EPO <u>Content/transaction data</u> Issuing or validation by Court/Judge <u>Subscriber/Access data</u> May be issued by prosecutors EPO-PR May be issued Prosecutors	EPO/EPO-PR **In principle same oversight** issuing authority can derogate for <u>subscribers or access data</u> in cases of established emergency **No issuing if issuing authority** has indications that: o Contrary to *ne bis in idem* o Issued for execution of a sentence or detention order rendered *in absentia* o For executing incoming MLA-requests from 3rd country	EPO <u>Content/traffic data</u> Issuing or validation by Court/Judge <u>Subscriber data</u> May be issued by ***independent*** prosecutors EPO-PR issuing authority must be ***independent*** Prosecutors

Table 2. Ex ante involvement of judicial authorities in member states different from issuing one

COM Proposal	Council GA	EP (Sippel Report)
Clarification through consultation o **EPO** for **access, transactional** and **content** data o **Reasons** to believe EPO affect other MS rules on immunities, privileges; freedom press/expression; security/defence o If consultation shows that EPO for **access, transactional** and **content** data would impact, issuing authority shall not issue	**Clarification through consultation** o **EPO transactional data** if subject resident another MS o **Reasonable grounds** EPO affect other MS immunities, privileges; freedom of press/expression; security/defence interests **Notification** o **Limited - Only EPO content data** and **if data subject** resident of other MS o **No suspensive effect**	**Systematic notification for all EPOs** o **1) Executing MS** of the service provider) **can** raise grounds of refusal (e.g. human rights, privileges and immunities) o **2) Affected MS** of Residence of the subject concerned **can** raise objections (e.g. essential interests - targeted person is a residing agent; trade secrets target is a business executive)

Source: authors' elaboration.

Originally scheduled for late March 2020, the vote of the LIBE Committee on the Report on the e-evidence file has been postponed for public health reasons linked to the Covid-19 crisis. Corona-related precautionary measures had a significant impact on the normal working activities of the European Parliament. They inter alia led the LIBE Committee to readjust its working calendar, and to draw up a list of files to be prioritised. The e-evidence files have allegedly not been included in such a list. To date, in fact, the work of the EU legislators on the proposed Regulation on European Production and Preservation Orders has not yet restarted, nor a date for the Committee vote on the file yet scheduled.

The Task Force discussions have highlighted how, besides disrupting the daily work of EU institutions on the e-evidence files, the Covid-19 crisis imposes the necessity of a thorough constitutional and legal assessment of the proposed e-evidence rules and of their multilevel impacts (on the systems for intra EU and international criminal justice cooperation, on individuals' rights and freedoms, and on different categories of service providers).

Civil society organisations that are members of the Task Force (including inter alia Fair Trials Europe and Privacy International) observed that since the start of the pandemic a wide range of states (including EU countries affected by rule of law threats) have increased the use of digital technologies for the purpose of performing surveillance activities, and enforcing new criminal offences and measures brought in haste. Introduction of broad emergency powers has usually occurred with limited legislative scrutiny. This is giving rise to legal uncertainty, with reported cases of misuse/abuse of the new digital surveillance and investigative powers and threats to the rule of law.[145]

Within Europe, for instance, Bulgaria has introduced new offences such as violation of quarantine measures and releasing 'false news' which might cause panic. The punishment is up to five years' imprisonment, and prosecutions have started – including against two doctors who complained that they are lacking masks and protective clothing. Linked with this new sanction, a new law has been approved in March 2020 by the Bulgarian Parliament giving the police the power to demand from providers of electronic services information related to their clients' use of services, without approval of the courts. The stated aim is to help the police control the location of the people under quarantine, but this occurs without the introduction of checks and balances to ensure that the police do not misuse this power.

Monitoring and quarantine enforcement apps have already been introduced in some member states (Poland, for example), and government authorities have made increasing use of telecommunication data held by telecommunications companies' operators. One Member of the European Parliament who took part in the Task Force meeting referred to the 'huge concerns' that members of the LIBE committee working within the Monitoring group on Rule of Law have expressed with regard to such developments.

[145] Mitsilegas, V. (2020), *Responding to Covid-19: Surveillance, Trust and the Rule of Law*, 26 May 2020.

5.3 Interlinkages with the external components of the package

The delay of the EU internal decision-making process on the proposal on e-evidence also has, in turn, far-reaching repercussions for the development of the international cooperation instruments on cross-border data access that the Commission is mandated to negotiate in the context of the Council of Europe Second Additional Protocol to the Cybercrime Convention, as well as – at the bilateral level – with the US.[146]

The Negotiating Directives annexed to the two different Council Decisions authorising the Commission to participate in these international negotiations expressly mention the e-evidence legislative proposals as a reference point for EU negotiations with the US and in the CoE context. However, the Task Force members expressed serious concerns regarding the possibility and opportunity for the EU to conduct external negotiations (e.g. with the US) on new international agreements on cross-border data gathering in criminal proceedings based on the proposed internal rules on e-evidence.

The July 2020 pronouncement of the CJEU in the *Schrems II* case had laid bare the impossibility of developing new international cooperation instruments allowing third counties which do not comply with EU data protection standards to directly obtain access to EU data, without the systematic involvement of EU oversight authorities. As it clearly emerges from the recent Court judgment, the latter have a crucial role to play to verify that transfers of EU data to third countries' authorities do not jeopardise the effective protection of EU fundamental rights.

Senior EU officials heard in the context of the Task Force referred to how negotiations with the US have been 'put on hold' and, reportedly, no further official meetings or significant developments have occurred since the EU-US Senior Officials meeting that took place at the beginning of March 2020 under the auspices of the Croatian Presidency. As for the Second Additional Protocol to the Budapest Convention, a negotiations round is reportedly scheduled for late October 2020.

The Task Force discussions have made clear that in a context where the processes of rule of law deterioration are accelerating in several EU countries, and where the adequacy of third countries' legislation and practices on data processing by law enforcement authorities are found incompatible with EU fundamental rights standards, there is a serious need for a thorough reassessment of the necessity and appropriateness of EU internal and external legislation introducing new cross-border data-gathering instruments outside existing judicial cooperation channels.

Such reassessment appears even more crucial in light of the shortcomings affecting: the evidence base required to justify the need for the different instruments proposed; the factors of constitutional and legal uncertainty still surrounding the different e-evidence proposals; and the doubts related to their actual added value for all the concerned stakeholders.

[146] Council of the European Union (2019), Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters. Brussels, 21 May 2019.

6. THE E-EVIDENCE PROPOSAL:
FACTORS OF LEGAL UNCERTAINTY

6.1 Lack of evidence showing need for new cross-border instruments

To date, there is no conclusive quantitative or qualitative evidence showing that existing instruments of judicial cooperation are unsuited to the specifics of cross-border data gathering for criminal justice purposes. On the contrary, Task Force discussions have identified several gaps in the knowledge needed to demonstrate the need for the e-evidence proposal.

At the national level, member states do not generally have a system for collecting and reporting information related to issued/received cross-border data requests, channels/instruments used, and related outcomes. There are important transparency deficits regarding the ways in which requests for different categories of data are issued, transmitted and executed by competent national authorities.

At the EU level, the Impact Assessment accompanying the e-evidence proposal does not give a complete overview of the current uses and outcomes of different cross-border data-gathering instruments. The Commission acknowledges that more data is needed and stressed that the Impact Assessment is only the 'starting point'. As for intra-EU cooperation, a particularly important gap is the implementation report of the EIO (originally due in May 2019), which has still not been produced. During the first meeting of the Task Force, the Commission stressed that a consultation exercise related to the use of the EIO, including in the field of cross-border data gathering, has been conducted with all participating member states. The Commission indicated that the EIO implementation report will be finalised by the end of 2020.

At the transatlantic level, the EU is seeking support from US authorities in collecting data that it can use to exactly quantify the time needed to execute a transatlantic data request through the EU-US MLA cooperation framework.

At the private sector level, the transparency reports produced by service providers use different reporting methodologies. Not all different categories of service providers concerned by the draft e-evidence legislation produce transparency reports. Furthermore, the transparency reports published by the main service providers (Facebook, Google, Microsoft, Twitter and Apple) generally do not indicate whether data-gathering measures are executed based on direct cooperation requests or following formal judicial cooperation procedures (e.g. MLAs).

The Task Force discussion furthermore highlighted the lack of a common understanding of how 'success' in the field of criminal justice cooperation for cross-border data gathering should be measured. It was observed that the speed of data-gathering processes cannot be relied on as the most important indicator of effectiveness.

A legislative framework that privileges direct public-private cross-border cooperation, with the objective of speeding up the gathering of data, might generate tensions with the need to secure basic rule of law safeguards and fundamental rights protections. The increasing demand for cross-border data does not automatically justify giving up systematic legality checks in the countries concerned.

6.2 The need for independent judicial oversight at the issuing/validation phase

Legal certainty can only be ensured in the presence of normative provisions capable of effectively requiring that a strict ex ante legality, necessity and proportionality assessment is conducted by competent judicial authorities in the issuing and/or validating state.

A wide consensus emerged among the Task Force members for the need to take into account the guidance and benchmarks provided by the CJEU on the level of judicial oversight and judicial protection required when issuing/validating criminal justice measures affecting different categories of fundamental rights. These include not only the rights to privacy and data protection, but also fair-trial rights. Concerns have been raised, however, by several Task Force members about whether the Commission and Council proposals would allow an adequate level of effective judicial protection in the country of issue.

In its proposal for an e-evidence regulation, the Commission suggests introducing common minimum standards of judicial oversight. Under the proposal, independent judicial scrutiny would be required to issue and/or validate production orders targeting content and transactional data. However, production orders targeting access and subscriber information, as well as preservation orders, could be issued directly by prosecutors.

The Council's general approach is, in principle, aligned with the Commission's proposed level of judicial oversight at the issuing stage. However, important derogations to the judicial validation requirements are foreseen when access to subscriber and access data is sought. It is in fact envisaged that orders may need to be issued directly by the police when the issuing authority establishes an emergency case and it is not possible to obtain the judicial authority's validation in time, particularly if the authority cannot be reached and an imminent threat requires immediate action. These provisions seem to leave a large margin of discretion to national authorities – that do not qualify as independent (judicial or administrative) – to determine and assess whether the urgency exists, and whether it justifies issuing orders without prior independent judicial validation.

To the extent that they allow EPOs and EPO-PRs to be issued directly by prosecutors, the Commission and Council proposals fall short of the EU legal benchmarks on 'independent' judicial oversight in the issuing member states. The risk exists that these measures are issued by judicial authorities that are: a) not independent from the executive (i.e. Ministry of Justice); or b) not independent or different from the judicial authority in charge of the prosecution. In the first circumstance, the issuing of an EPO/EPO-PR would run counter the CJEU jurisprudence (and its line of cases on the EAW) on who qualifies as an 'issuing judicial authority' in mutual recognition proceedings. In the second circumstance, there is a concrete possibility that the effective protection of data subject and/or suspect and accused persons' fundamental rights is

undermined (as indicated by the two different opinions recently issued by the CJEU Advocate Generals on the concept of judicial authority in the EIO Directive).

The judicial authorities that are competent for the issuing of investigative measures entailing interference with the fundamental rights to privacy or data protection vary significantly across the EU member states. While some member states allow the production of certain categories of metadata to be ordered directly by prosecutors, in some EU countries a validation by an independent judge is needed even for the issuing or validation of an order mandating the production of subscriber information. This happens, for instance, when such a measure is considered to affect fundamental rights of the data subject. Under the Commission and Council proposals, the possibility exists that an EPO targeting subscriber and/or access data issued and/or validated by prosecutors is addressed directly to service providers in member states where a higher level of judicial protection is required.

At the same time, the sizeable possibilities that the proposed instruments would provide to prosecuting and investigating authorities are not tempered by dual criminality requirements (dual criminality constitutes grounds for refusal instead under the EIO Directive, although only optional and restricted to non-list offences).

Doubts about the compatibility of an EPO or EPO-PR with rules and obligations deriving from EU, international or national criminal or privacy laws might, in turn, lead service providers to challenge the data-gathering measures in national or European courts. It was pointed out that litigation might become a way for companies to not only protect customers against potentially abusive orders, but also to avoid legal responsibilities and related financial liabilities that could result from executing a measure that conflicts with other privacy and criminal justice rules.

The Sippel Report proposes an overall increase in the level of independent judicial oversight required to issue all the different types of orders envisaged. It does so in particular by suggesting that production orders targeting content and traffic data (including access data) should be issued or validated by an independent court or a judge. The rapporteur foresees the possibility for production orders targeting subscriber data, as well as preservation orders, to be issued by prosecutors, but only if the latter meet certain judicial independence standards. According to the Sippel Report, a prosecutor should be considered independent if he/she is not at risk of being exposed – directly or indirectly – to directions or instructions from the executive, such as a Minister for Justice, in connection with the adoption of a decision in a specific case. The rationale behind this proposal is to align the regulation with recent CJEU case law.[147]

6.3 Lack of involvement of competent judicial authorities in member state of execution and/or in the affected member state

Contrary to existing instruments of intra-EU and international judicial cooperation in criminal matters, the Commission's proposal for a new e-evidence regulation would not require the systematic ex ante involvement of the judicial authorities in the country of execution. The latter would be de jure and de facto prevented from raising non-recognition grounds. They are in fact

[147] See, for instance, Minister for Justice and Equality v OG and PI.

only required to take part in the execution procedure when it is necessary to enforce the issuing state's order due to the private company objecting.

The main addition proposed by the Council in its general approach is a notification mechanism that could be activated by the issuing authority on the adoption of production orders targeting content data. However, several Task Force members (including prosecutors, criminal lawyers, academics and private sector representatives) have expressed concerns about the limitations of the notification mechanism envisaged in the general approach. These concerns include the mechanism's limited scope, since it is only for production orders targeting content data. Also, it would not allow the country of execution to suspend or prevent the enforcement of an order, even when the latter is found to be incompatible with the fundamental rights, legal professional privilege/professional secrecy, and national security interests protected in the country of execution.

The Sippel Report proposes the introduction of systematic notifications to both the affected state and the state of execution concerned by production orders. Contrary to the notification system proposed by the Council, those envisaged by the rapporteur would only allow the execution of production orders by a service provider *if* the notified member states do not raise any grounds for refusal.

At the same time, the notification system included in the Sippel Report still leaves the possibility that a notified country does not object to the execution of orders, even when they should have done so, for instance, to prevent the execution of an order which runs counter to fundamental rights or rule of law safeguards provided under EU law. This means the notification mechanisms foreseen in Sippel's proposal would not systematically prevent conflicts of laws and fundamental rights issues that could still arise in the event that either the 'member state of execution' or the 'affected member state' remain silent after receiving the notification.

Furthermore, some Task Force members noted that the lack of an explicit obligation of the judicial authority in the executing state to formally authorise the data transfer (and thus inform the provider after examination that the request is valid) deprives providers from legal certainty before handing over the data to the issuing authority.

It therefore appears that none of the different proposals guarantee a systematic and/or meaningful involvement of the member state of execution (nor of the affected member state) which would effectively qualify as a form of judicial cooperation satisfying EU fair-trial standards in the criminal justice domain. Serious doubts exist as to whether limiting the involvement of second EU member states' judicial authority to (various forms of) notification is in line with EU and member states' constitutional judicial protection requirements.

The lack of recognition of a criminal justice decision by competent judicial authorities in the second (executing or affected) member state would fail to qualify the proposed measure as a form of judicial cooperation in criminal matters. In the EU criminal justice area, mutual trust must be ensured between judicial authorities. The latter are responsible for enforcing criminal jurisdiction, as well as for making sure that the issue *and* execution of a criminal justice decision under existing mutual recognition instruments does not result in abuses of fundamental rights (or at least their core essence) as protected at EU and national constitution level.

By giving away systematic ex ante involvement of and prior validation by the second member states' judicial authorities in the recognition phase, the e-evidence proposal would put the companies at the centre of mutual-recognition proceedings.

During the Task Force meetings, service providers expressed concerns regarding the actual possibility and specific circumstances under which they could or should challenge the legality and/or proportionality of measures, or flag risks of potential conflicts of laws. In particular, criticisms were expressed towards the Council's general approach, according to which service providers should not be allowed to object to executing a received order, even if the measure appears to be manifestly abusive in light of the EU Charter of Fundamental Rights. It was also noted that the limited information included in the certificate accompanying the data-gathering measure would de facto prevent service providers from identifying and raising issues related to the received order (e.g. existence of legal professional privilege/professional secrecy).

6.4 Incompatibility of public-private partnerships with EU criminal justice *acquis*

The measures envisaged by the e-evidence proposal would grant investigating and prosecuting authorities the powers to directly order the preservation and production of different categories of sensitive information (including content) held by service providers across borders. This would mean adopting a model of public-private partnership in the fight against crime that is extraneous to the constitutional and legal frameworks that govern criminal justice and police cooperation in the EU legal system.

Task Force discussions on the EU legal constitutional framework on judicial cooperation highlighted a number of doubts concerning the choice of Article 82.1 of the TFEU as the legal basis for the proposed e-evidence regulation. These doubts chiefly relate to the lack of meaningful involvement of second judicial authorities, and the possibility of qualifying a form of direct cross-border cooperation between judicial actors and private companies as 'mutual recognition in criminal matters'.

Direct cross-border cooperation between law enforcement authorities and service providers abroad is currently explicitly allowed under US law. However, within the EU legal system, the scope for direct cooperation between investigating/prosecuting authorities and service providers is extremely limited.

As clearly stressed by the CJEU, companies under EU jurisdiction can only provide access to communication data sought for law-enforcement purposes in cases where a prior review has been "carried out by a court or an independent administrative body, following a reasoned request of [competent national] authorities submitted within the framework of procedures of prevention, detection or criminal prosecution." This requirement can in principle be waived only in cases of "validly established urgency".[148]

Prior validation by an independent administrative and/or judicial authority in the country of execution is crucial to secure legal certainty and protection to concerned individuals (suspect

[148] Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB.

and accused persons, and data subjects) as well as private companies. This type of systematic involvement of competent authorities in the country of execution is designed to compensate for the disparities in levels of protection and safeguards (e.g. on privacy, data protection, and fair-trial rights) that currently persist between EU member states and third countries, including the US.

As far as intra-EU cooperation is concerned, a high level of fragmentation and disparity also still exists among members states' criminal justice and law enforcement systems. Clear examples of this can be seen in the persistent lack of harmonisation in rules on the admissibility of criminal evidence, and the inconsistent implementation of the EU procedural rights *acquis* in criminal proceedings (e.g. Directive on Access to a Lawyer), as well as uneven detention conditions regimes and standards across member states.

Extending US law enforcement's modus operandi to intra-EU and international cooperation risks undermining the consistent application of EU law that applies to access to data for law enforcement and criminal justice purposes. This is especially true considering the wide scope of application of orders envisaged under the proposed e-evidence rules, both in terms of categories of service providers concerned, and the crimes covered.

6.5 Limited access to effective remedies and fair-trial risks

The lack of (systematic and/or meaningful) involvement of the competent oversight authorities in the executing or affected states has far-reaching repercussions for legal certainty. This is because it limits the right to an effective remedy that EU law grants to suspects and accused persons, as well as to concerned third parties whose rights might be affected by the execution of a data-gathering measure.

When an order concerns a person who does not reside in the issuing state, the executing state, or member state of residence or citizenship, is by default better placed to verify the existence of such issues or privileges. In particular, the ex ante intervention of an independent judicial authority in the executing state remains crucial for upholding fair-trial principles. Without the opportunity to seek remedies in the executing state, the risk exists of increasing appeals against companies through civil law, which do not qualify as effective remedies in criminal justice.

Clear rules on notification to the persons whose data are held/processed (especially when it comes to third parties) has been identified as a central requirement for any regulatory framework dealing with criminal justice cooperation. Representatives of the private sector, as well as defence lawyers who took part in the Task Force meetings, stressed that the proposal needs to include provisions capable of indicating and clarifying the exact grounds on which EPOs should be kept secret in order not to jeopardise an investigation. During the pre-trial phase, the secrecy of a data-gathering measure might be justified. If so, notifying the person concerned by the proposed measures remains a crucial condition to ensure that access to remedies is possible in the trial phase.

Some members noted that the proposed e-evidence regulation does not exactly specify what type of information needs to be disclosed to the defence (and to the court). To ensure defence

rights in criminal proceedings, this information should include the basis for request, the search that was done, and the way that the data was analysed by investigating/prosecuting authorities.

Important concerns have been raised by defence lawyers in relation not only to the guarantees of fair-trial rights, but also to the need to preserve legal professional privilege/professional secrecy. In fact, as one Task Force member noted, professional secrecy is not only an essential element of the right to a fair trial (Article 6 of the European Convention on Human Rights - ECHR) but is also protected by the right to respect for private and family life (ECHR Article 9).

It was also observed that fundamental rights' issues, and tensions with the need to guarantee immunities and legal professional privilege/professional secrecy, are likely when only limited information is included in the certificates accompanying the proposed orders. Companies know their data; they understand what a proportionate request is and the implications of keeping a data request secret. A clear example of this interlinked issued is the need to safeguard legal professional privilege/professional secrecy.

6.6 Sanctions for non-compliance, and reimbursement of costs

The imposition of sanctions in cases of non-compliance, and the reimbursement of costs incurred executing the proposed orders, emerged as important practical issues.

Private sector representatives are concerned that financial penalties for cases of non-compliance should be proportionate. The definition of fines and the determination of their amounts also have far-reaching privacy and criminal justice repercussions. If sanctions are too high (as potentially foreseen in the Council's general approach), they might have a 'cooling' effect on service providers. The latter could thus become 'passive' recipients of fundamental rights-sensitive criminal justice measures, and feel compelled to execute orders even when they should not have done so. This is especially the case for ISPs with only a limited number of employees and lacking the financial or human resources to carry out difficult legal assessments and to establish whether it is opportune or necessary to object to the execution of an order.

The Task Force members highlighted the crucial importance of including clear and harmonised rules on reimbursement of costs. Several service providers are concerned by the possibility of having to support the costs of executing potentially high volumes of orders, while at the same time having to seek reimbursement in the country of issue (i.e. in a different country to the one where they are established or provide their services). Precise rules on reimbursement of costs associated with the execution of the proposed order are critical to prevent the measures from having a negative economic impact on service providers. It was furthermore noted that precise and transparent rules on cost reimbursement can act as a cooling factor for issuing authorities, and help prevent them from issuing orders by default, including for minor offences.

As for the obligation to appoint a legal representative, the EP rapporteur proposes that this should only apply to service providers not established in the EU, or to EU service providers established in an EU member state not participating in the regulation but offering services in the participating member states. Such a proposal is linked with a specific understanding of when an order should be considered purely as domestic or when it amounts to a cross-border measure. According to the EP Report, as soon as the data are abroad the case is no longer exclusively domestic.

7. DOUBTS ABOUT THE E-EVIDENCE INITIATIVE'S ADDED VALUE

7.1 From the perspective of criminal justice actors

The orders envisaged by the Commission's e-evidence proposal have been presented as measures mainly intended to tackle serious crime and terrorism. In terms of specification of the offences for which EPOs could be issued, the Commission's proposal and the Council's general approach differ from the sentencing thresholds suggested by the rapporteur. The Sippel Report proposes increasing the sentencing threshold required to issue production orders targeting content and traffic data (to five years). Such a threshold, however, would not apply to offences for which evidence is mostly available in electronic form; nor would the additional terrorism-related offences described in the Directive 2017/541/EU require the minimum threshold of five years.

Members noted that introducing an overly broad instrument (in terms of crime covered) will likely lead to a default utilisation of the proposed orders. However, fostering a law-enforcement and policing approach to cross-border data gathering is likely to be detrimental for several reasons.

Expanding the scope for investigating and prosecuting authorities to issue orders is likely to lead to an increase in the administrative burden on national judicial systems, with judicial authorities potentially needing to review large numbers of orders.

There is a risk of reducing the quality of requests for data. Not only does the issuing of data-gathering measures often require specific legal and technical competences, it also must always be proportionate to the objectives pursued.[149] There will be more time pressure on criminal justice oversight actors (i.e. courts and judges), which risks undermining their capacity to effectively carry out an independent and impartial review of the proposed measure (in both the issuing and executing country). Furthermore, it is not clear how the potentially high volumes of 'raw' data obtained will be dealt with.

Doubts about the compatibility of an EPO or EPO-PR with rules and obligations deriving from EU, international or national criminal and privacy laws might lead service providers to challenge the measures in national or European courts. It was pointed out that litigation might become a way for companies to not only protect customers against potentially abusive orders, but also to avoid legal responsibilities and related financial liabilities that could result from executing a measure in conflict with other applicable privacy and criminal justice rules. Meanwhile, conflicts of law would still arise in the case of EPOs targeting content data held by service providers with 'US citizenship'.

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

Legal practitioners — including both prosecutors and criminal lawyers — who are members of the Task Force noted that designing provisions capable of ensuring the lawful cross-border and cross-jurisdictional collection and exchange of data is also in the utmost interest of prosecutors. The ultimate priority of the latter is to ensure that information collected from service providers across borders is admitted as evidence in court.

That notwithstanding, it is clear that data obtained through the proposed orders could still be used, not only as a source of intelligence by law enforcement authorities (e.g. to create 'parallel evidentiary constructions') but also as evidence in court. Some members noted that exclusionary rules for unlawfully collected data appear to be an exception in European legal systems. Even when such rules exist, they are limited in scope. Furthermore, there are still no common EU standards on admissibility of evidence. To date, the European Court of Human Rights' guidance on exclusion of evidence is very limited (only covering evidence acquired via torture). Against this backdrop, the risk exists that data collected unlawfully across borders could still be admitted as evidence before a court in the EU country issuing an EPO/EPO-PR.

7.2 From the perspective of service providers

The Task Force discussions highlighted how the added value of the different components of the e-evidence package has not been demonstrated equally for all stakeholders concerned by the proposed measures. The actual capacity of different private companies to fulfil tasks and duties and to exercise rights under the proposed e-evidence legislation would differ significantly depending on a number of factors. These would include the type of services offered, as well as the size of the provider, the country of establishment, and the subjection to different national and supranational criminal justice and privacy law frameworks.

Several service providers are concerned by the possibility of having to cover the costs associated with executing potentially high volumes of orders, while at the same time having to claim and seek the reimbursement of costs in the country of issue (i.e. in a different country to the one where they are established or provide their services).

The Task Force members highlighted the crucial importance of including clear and harmonised rules on reimbursement of costs associated with executing the proposed orders which are critical to prevent the measures having a negative economic impact on service providers. It was furthermore noted that precise and transparent rules on cost reimbursement can act as a cooling factor for issuing authorities and help prevent them issuing orders by default, including for minor offences.

The definition of fines and the determination of their amounts have far-reaching privacy and criminal justice repercussions. If sanctions are too high (as potentially foreseen in the Council's general approach), they might have a 'cooling' effect on service providers. The latter could thus become 'passive' recipients of fundamental rights-sensitive criminal justice measures, and feel compelled to execute orders even when they should not do so. This is especially the case for ISPs with only a limited number of employees and lacking the financial or human resources needed to carry out difficult legal assessments and to establish whether or not it is opportune or necessary to object to an order.

7.2.1 US internet and cloud service providers

From the perspective of providers of cloud and internet services which have 'US citizenship' but also deliver services in the EU, the e-evidence initiative recognised the need to establish a clear international legal framework for transatlantic data access in criminal matters.

Cooperation between EU authorities and US companies currently takes place on a voluntary basis and is limited in scope, being restricted to disclosure of non-content data which do not pertain to US persons. The proposed e-evidence regulation would empower EU investigators and prosecutors to address EPOs and EPO-PRs (including for content data) directly to US cloud and internet service providers. The latter would, however, still remain subject to US criminal and privacy laws, which currently prevent service providers under US jurisdiction from disclosing content data directly to foreign authorities.

From the perspective of providers of cloud and internet services which have 'US citizenship' but also deliver services in the EU, the added value of the regulation would therefore not be automatically assured. In fact, a new EU instrument allowing members states' judicial authorities to order the production of content data directly to US service providers would not prevent conflicts of law and jurisdictions at the transatlantic level.

Conflicts of law and jurisdiction at the transatlantic level could only be systematically prevented through the conclusion of an international agreement on cross-border data access between the EU and the US. This is provided that such an agreement complies with the constitutional and legal requirements that, under EU law, govern the gathering of electronic data for criminal justice and law enforcement purposes.

Discussions related to the types, scope and levels of fundamental rights safeguards to be guaranteed in transatlantic cooperation on cross-border access to data for criminal justice purposes have been at the centre of the negotiations of the "EU-US Agreement to facilitate access to electronic evidence in criminal investigations". Available documents show how divergences between the parties relate to the exact content and scope of procedural safeguards, as well as privacy and data protection requirements that should be included in the agreement.

During the first negotiation rounds, the US asked the Commission to provide clarifications related inter alia to: non-discrimination requirements under EU law; the exclusion from the scope of the agreement of data covered by the essential interests of a member state; data protection safeguards; and requirements related to notification, judicial review, targeting restrictions and minimisation. The Commission, for its part, raised concerns about the possibility that data may be requested by US authorities for criminal proceedings that could lead to the death penalty.

Discussions on such points had to deepen in the following negotiation rounds. The Commission, for instance, needed to stress that certain categories of data (i.e. transactional data, according to the new category introduced in the proposed e-evidence regulation) cannot be granted a lower level of protection than that guaranteed to content data under EU law. The Commission also reminded of the importance of an independent assessment and the involvement of judicial

authority. Such a reminder seems to refer to the level of judicial oversight foreseen for the issue of production and preservation orders under the Commission's e-evidence proposal. However, the European Parliament Report on the e-evidence file foresees that a higher level of independent judicial scrutiny should be granted by the issuing state.

In any case, and at least as far as subscriber information is concerned, both the Commission proposal and the EP report require a higher level of judicial oversight than that foreseen under US law. The Commission had to ask for further information on the role and involvement of judicial authorities in the US criminal law system. Applicable judicial redress standards under US law (i.e. under the US Judicial Redress Act) and data protection remedies available in that country were also discussed in the following negotiating rounds, in particular, it seems, to assess their compatibility with EU law requirements.

While underlining the need for strong privacy and data protection safeguards (e.g. the application of the Umbrella Agreement), the Commission's report on the second round of negotiations still supports the model of direct cooperation with service providers. Such an approach, however, is currently not allowed for EU cooperation on cross-border evidence gathering in criminal matters, and found strong resistance within the EU as far as intra-EU cooperation is concerned.

As one of the speakers noted during the last Task Force meeting, the transatlantic negotiations were delayed due to the coronavirus outbreak, but not only because of that. Other delaying factors appear to have been the EP's calls for further scrutiny and reflection over the proposed EU internal rules on e-evidence, as well as the differences of views over the specific types and level of safeguard that the two parties consider necessary.

Doubts also persist with regard to the envisaged 'architecture' of the agreement. During one of the Task Force meetings, an EP representative raised questions with regard to the form envisaged by the Commission for the future EU-US agreement. It was noted that the conclusion of a 'self-standing' EU agreement would be more appropriate to the post-Lisbon Treaty framework, where the EU acquired (exclusive) external competences in judicial cooperation in criminal matters. Such a solution could also increase intra-EU coherence and consistency in the application and implementation of the future framework of cooperation, and 'make up' for the absence of bilateral agreements between the US and single member states.

7.2.2 Telecommunications companies

Clear indications of how the measures would improve cooperation with EU investigating and prosecuting authorities are lacking for telecommunications companies in EU member states. Representatives of this category of service provider stressed that they can already count on well-established and functioning forms of cooperation with the national authorities of their country of establishment. According to representatives of the telecoms sectors, orders for the production and preservation of data received by telecommunications operators are currently answered in a timely and adequate manner.

In the Commission's Impact Assessment, the estimation of the 'magnitude of the problem' (i.e. number of cross-border requests for data not executed, or not executed at the right time) is

based on two basic sources of information: the result of a survey of member states' authorities, and the transparency reports of the main US service providers (Facebook, Google, Microsoft, Twitter and Apple). In the Impact Assessment there is, however, no reference to transparency reports prepared by telecommunications operators.

According to representatives of the telecoms sectors, requests addressed to telecommunications operators are answered in a timely and adequate manner. Therefore, it was noted how the Impact Assessment does not provide enough evidence to fully justify the e-evidence proposal for all the different categories of service provider concerned.

7.2.3 Small and medium service providers

Small and medium enterprises (SMEs) providing internet services might have a lot of customers, and therefore control high volumes of data. Nevertheless, companies with only a very limited number of employees simply lack the organisational capacity and in-house legal expertise needed to promptly react to direct orders for production of different categories of data, and to effectively verify the existence of grounds for raising legitimate (fundamental rights or conflicts of laws) objections. The six-hour deadline to comply with an emergency request was described as 'completely unrealistic' for most SMEs.

Doubts were raised over whether the private sector has the resources needed to cope with the potentially high numbers of requests. Private sector representatives who took part in the kick-off meeting stressed that, on receiving a direct cross-border request for data, they often have to invest time and effort in verifying whether the measure has been issued or validated in the issuing country by a competent authority.

Some Task Force members argued that the Commission proposal is essentially a solution to a financial problem. Most notably, they suggested it constitutes a way to address the limited capacity and willingness of member states and third countries to allocate sufficient resources to responding in good time to incoming cross-border data requests. This argument is linked with the issue of prioritisation of financial resources to improve mutual legal assistance (MLA) procedures, which has also been identified as a key factor to consider.

The Task Force research has shown that the processes for extracting and handing over data can be quick for certain categories of electronic information (e.g. basic subscriber information). Also, it emerged how the formalisation and automatisation of processes through digital communication and data exchange platforms (such as the ones established at the domestic level by several EU member states) between authorities and service providers under their jurisdiction can significantly help reduce times for data handovers.

However, proposals for instruments introducing time limits within which service providers are obliged to materially execute a production order cannot disregard the fact that retrieving, extracting and producing the data sought involves certain technical and operational delays.

PART IV:
WAYS FORWARD WITHIN THE EU AND ACROSS THE ATLANTIC

8. STRENGTHEN EXISTING INSTRUMENTS OF JUDICIAL COOPERATION FOR DATA GATHERING WITHIN THE EU

The EU's current instruments of judicial cooperation are the European Investigation Order (EIO) and mutual legal assistance (MLA) agreements. While enabling the cross-border collection and exchange of data in criminal matters, these also meet the objective of preserving legal certainty and preventing conflicts of law, both within the EU and in cooperation with third countries.

A key feature of these instruments is the systematic and effective scrutiny and validation of investigative measures by judicial authorities in the country where the measures are to be executed. Such involvement allows trust and legal certainty to be maintained within the EU and across the Atlantic. It ensures that the enforcement of criminal jurisdiction by foreign authorities is subject to reciprocal judicial scrutiny and does not translate into an unlawful infringement of EU and national constitutional rule of law and fundamental rights' standards.

8.1 Investing in the EIO

The EIO is progressively proving its added value as a judicial cooperation instrument, allowing member states' judges and prosecutors to swiftly request, collect and exchange different categories of information across the EU in line with the principle of mutual recognition of judicial decisions in criminal matters.

It is increasingly used by judicial authorities across the EU to gather a wide range of electronic information, including content of electronic communications, metadata and basic subscriber information.

The EIO ensures legal certainty for the service providers holding the data sought. Final addressees of the order can trust that investigative measures have been adopted following the right procedures. Thus they do not have to invest time and effort in verifying whether the measures have been issued or validated by an authority effectively competent to do so.

The EIO also works in urgent cases, with practitioners reporting that the issue, transmission and execution of data-gathering measures through an EIO can even occur 'in a matter of hours'. Real-time contact and cooperation between the judicial authorities in the member states issuing and executing an EIO (also in the phases before its issue) can be facilitated through Eurojust and the judicial authorities working at the National Desks of the countries concerned by an investigative measure. To further facilitate this type of cooperation, Eurojust could deliver streamlined guidelines on how urgent requests for cross-border data can be issued and executed through the EIO and MLA channels.

The EIO provides for access to effective criminal justice remedies. Suspects and accused persons can appeal before the judicial authorities of the executing state if it is deemed that the

production or preservation of data subject to an EIO has resulted in a breach of certain rights. The intervention of an independent judicial authority in the country of execution therefore constitutes a crucial *conditio sine qua non* for upholding the fair-trial principles laid down in the EU Charter of Fundamental Rights.

8.2 Independently evaluating and assessing the EIO

The EIO implementation report, initially due in May 2019, has not yet been published. To date, there is neither qualitative nor quantitative evidence supporting the Commission's claims that cooperation under the EIO generally takes too long and is therefore ineffective for the specific purpose of collecting data held across borders.

The Task Force discussions highlighted the urgent need for an independent evaluation of the EIO's implementation. Such an evaluation should focus especially on assessing the EIO functioning and outcomes with specific regard to judicial cooperation for cross-border border preservation and production of different categories of data.

While the Commission already requested an external evaluation of the EIO, an ex post impact assessment could also be performed under the initiative of the European Parliament (EP).

This assessment could help the EP verify how the EIO operates in practice. It would ensure adequate democratic scrutiny over the added value and effectiveness of this mutual recognition instrument, as well as the results achieved during its first phase of implementation.

The assessment could also help to precisely identify the judicial authorities competent for the issuing and/or validation of data-gathering measures in each member state, and assess whether their statutory requirements are up to EU standards on judicial independence.

The assessment would allow a country-by-country review of the minimum standards or thresholds (such as reasonable suspicion) that EU member states have in place to justify the issuing of such requests. It would also allow the EP to identify the different grounds/circumstances under which member states allow or require such measures to be kept secret in order not to jeopardise investigations. The assessment should furthermore take into account whether effective and enforceable data subject rights are guaranteed for data processing under the EIO system, in line with GDPR requirements.

An independent assessment of the EIO is also necessary to verify the extent to which 'delays' in cross-border data gathering are linked to the technical issues (e.g. complexity of technical processes and procedures that service providers have to implement) or the ways in which judicial cooperation currently takes place. It is also required to verify the quality of data currently obtained through the execution of EIOs. Ensuring the integrity and authenticity of the data that judicial authorities and/or lawyers receive pursuant to the execution of an EIO is key to securing chain of custody and fully respecting the rights of the defence.

A thorough independent assessment of the EIO would provide the evidence basis needed to develop targeted EU interventions to strengthen and streamline cooperation for cross-border collection of data under the EIO. These interventions could include specialised judicial training

programmes aimed at increasing the capacity of EU member states' competent authorities to formulate clear and complete requests for electronic data using the EIO forms.

8.3 Creating a mechanism to evaluate EU mutual recognition instruments in criminal matters

The EU legislator should establish a new mechanism for independently evaluating the function and implementation of EU policies and laws in the area of criminal justice. This is necessary to increase the transparency of how the need for new EU instruments of judicial cooperation in criminal matters is assessed.

Article 70 of the TFEU requires this evaluation mechanism to be designed in a way that allows for the objective and impartial evaluation of the implementation of EU criminal justice instruments (such as the EIO and MLAs) by EU member states' authorities. In particular, to facilitate "the full application of the principle of mutual recognition".

To increase effectiveness, objectivity and impartiality in the evaluation, the new mechanism should not only rely on periodic reviews by member states' authorities. It should also involve other institutional and societal stakeholders directly concerned by the practical implementation of EU instruments.

In the case of the EIO and the MLA, the evaluation should rely on the work and advice of EU agencies such as the Fundamental Rights Agency, and bodies such as the European Data Protection Supervisor.

It should also foresee the participation of internet and telecommunications service providers, which can count on a solid track record of cooperation with EU member states' investigating and prosecuting authorities. Private sector organisations have an important role to play in adequately assessing the different technical problems related to the execution of data requests, as well as in identifying possible solutions to such problems.

Defence lawyers and civil society actors could also contribute significantly to the effectiveness of evaluation mechanisms, in particular by fostering a better understanding of the rights and role of the defence in both issuing and executing countries. They can contribute by assessing the different ways in which the increasing use of information technologies in cross-border investigations can affect or foster the effectiveness of the procedural rights of suspects or accused persons. Most notably, their right to access a lawyer and an effective criminal defence.

8.4 Promoting digitalisation at the service of criminal justice

Utilising digital technologies should not mean sacrificing or sidelining the essential role of independent judicial authorities; rather it should facilitate their work.

New digital platforms are needed to foster communications and dialogue between member states' judicial authorities, and to allow them to exchange criminal justice decisions – most notably EIOs and MLA requests – in a secure, fast, streamlined and trusted way.

New technologies have the potential to render the process of cross-border gathering of data swifter, more transparent and reliable. These factors can significantly increase trust among judicial authorities, and speed up judicial cooperation, while at the same time preserving crucial EU fundamental rights and rule of law safeguards.

Within the EU, national platforms that allow investigating and prosecuting authorities to transmit data requests to private companies under their jurisdiction also allow for streamlined communication processes and a 'high degree of formalisation'. This applies to both the requests transmitted by investigating and prosecuting authorities, and the answers provided by companies. The creation of Single Points of Contact (SPOC) on both sides proved useful in eliminating ambiguities in the communication process, and significantly reduced 'turnaround times' of requests.

An EU-level platform for digital exchange of information and documents between competent judicial authorities is needed to complement national systems, and to improve cross-border judicial cooperation within the EU. Such a platform would facilitate the transmission of judicial orders, court decisions, translations, and data obtained from private companies executing an investigative measure.

It is therefore important to establish a single EU portal of communication and transmission of EIOs between competent judicial authorities. Without a secure transmission platform, and without secure and trusted communication platforms allowing dialogue and exchange of criminal justice decisions between competent authorities in member states, operators can face fines for not delivering on time.

The roll out of the e-Evidence Digital Exchange System (eEDES) aims precisely to implement an EU-wide platform for electronically exchanging data collected through the EIO and MLA instruments in a trusted, secure and admissible way, and through clear and standardised electronic forms (instead of personal email or postal service). The envisaged interface should be limited to communication and exchange of measures and data among competent EU judicial authorities, while access to such a platform should be guaranteed only for judicial authorities meeting minimum independence standards.

The eEDES system should include functionality allowing the clear identification – in both the issuing and executing states – of the specific judicial authorities competent to adopt and/or validate the different measures that can be included in an EIO. The system should also allow for the involvement of different judicial authorities when different investigative measures are included in a single EIO.

This new platform could significantly facilitate the work of investigating and prosecuting authorities, because it would allow the issuing and execution of a wide range of investigative actions (including orders mandating the cross-border production and preservation of data) through a single judicial tool. It gives rise to a complete, new and, above all, functional instrument of judicial cooperation.

The need for improved 'digital justice' solutions has become even more evident since the Covid-19 crisis, which has significantly impacted the functioning of criminal justice systems across

Europe and beyond. The digitalisation of justice (and in particular 'remote justice solutions') is known to have a negative impact on defence rights (e.g. right to lawyer, access to case file, presence at trial). Yet new infrastructures for digital communication among judicial authorities have the potential to make the current system of cross-border data gathering more secure, direct, transparent and effective.

If properly designed and implemented, a digital platform for securely communicating and exchanging data could not only speed up judicial cooperation in criminal matters, but also increase the personal safety of end users.

The digital exchange system being set up to transmit EIOs and MLAs between judicial authorities must be clearly distinguished from other platforms (existing or under development) that allow law enforcement authorities to request and obtain personal information from private companies. The direct interconnection of service providers with foreign authorities belonging to different constitutional and criminal law traditions is likely to generate new and largely unexplored challenges.

9. WITHDRAW THE EU PROPOSALS ON E-EVIDENCE

The e-evidence proposals should be withdrawn because they fail to meet normative standards and rule of law requirements. Compliance with these standards and requirements is necessary to justify the introduction of new instruments for cross-border data gathering in criminal matters, and to ensure their compatibility with the EU primary and secondary laws governing judicial cooperation in the EU criminal justice area.

9.1 Lack of evidence on the proposal's added value, necessity and proportionality

The added value, necessity and proportionality of the e-evidence proposals have not been demonstrated by the impact assessment accompanying them. The Task Force discussions clearly highlighted the negative implications of the proposed e-evidence rules, not only for service providers and judicial actors, but also suspects and accused persons, and third parties whose data might be targeted.

From the perspective of providers of cloud and internet services that have 'US citizenship' but also deliver services in the EU, the added value of the regulation would not be automatically ensured. Introducing a new EU instrument allowing member states' judicial authorities to order the production of content data directly from US service providers is only likely to multiply conflicts of laws and jurisdictions at the transatlantic level.

There are no indications that the proposed measures would improve cooperation between EU investigating/prosecuting authorities and telecoms companies operating in another EU member state. This category of service provider can already count on well-established and well-functioning forms of cooperation with the national authorities of their country of establishment. According to representatives of the telecoms sector, orders for the production and preservation of data received by telecoms operators are currently answered in a timely and adequate manner.

SMEs simply lack the organisational capacity and in-house legal expertise to respond promptly to orders for the production of different categories of data, while at the same time verifying the grounds for raising legitimate (fundamental rights or conflicts of laws) objections. The six-hour deadline for complying with emergency requests was described as "completely unrealistic" for most SMEs.

By privileging a law-enforcement and policing approach to cross-border data gathering in criminal matters, the proposed e-evidence measures are likely to increase time pressure on judicial oversight actors (i.e. courts and judges). They also risk undermining these actors' capacity to effectively carry out an independent and impartial review of the proposed measure (in both the issuing and executing country).

9.2 Incompatibility with principles and rules governing criminal justice cooperation

The proposed e-evidence rules would undermine the correct application of the principle of mutual recognition within the EU criminal justice area, since direct public-private cooperation cannot be framed as a form of judicial cooperation under EU law as foreseen in Article 82 of the TFEU.

The existing mutual recognition instruments provide for judicial protection in both the issuing and the executing member state. The e-evidence proposals eliminate the standards under the law of the executing member state. The proposed cooperation mechanism thereby deprives the individual of the protection of his/her privacy rights under the law of the executing state. This lack of protection cannot be compensated by judicial control in the issuing member state because the authorities of the latter lack the expertise to apply foreign law and will not be aware of potential violations of the rights of the individual concerned. Judicial oversight by the issuing member state alone cannot offset the elimination of the standards of protection provided by the executing member state.

Service providers cannot be responsible for verifying the necessity or proportionality of criminal justice measures, nor can they be expected to verify the legality of acts based on the different legal systems of all EU member states. For such complex issues – which bring the risk of breaching the rule of law – an independent judicial authority in the provider's state must be responsible. The authorities of the executing member states need to remain in charge of the legal assessment of any order received from other member states, before transmitting the validation to the service provider for execution.

None of the different proposals advanced can guarantee a systematic and/or meaningful involvement of the member state of execution (nor of the 'affected member state') that effectively qualifies as a form of judicial cooperation satisfying EU fair-trial standards.

Even when compulsory and systematic, a system of 'mutual notification' (as opposed to recognition) would not prevent possible conflicts of laws and fundamental rights issues that could still arise if either the member state of execution or the affected member state remains silent after receiving the notification. Such a notification system would not meet the high standards of judicial control that the CJEU has found to be required over both the issue *and* execution of cross-border criminal justice measures.

The systematic review and formal validation of cross-border investigative measures by an independent judicial or administrative authority in the country of execution is a key feature of the EU system of judicial cooperation in criminal matters.

Bypassing such involvement responds to a policing and law-enforcement approach that prioritises fast and direct access to data. Yet it is incompatible with the objective of respecting the legal processes and safeguards applying to EU criminal justice cooperation in the field of cross-border evidence gathering. This kind of approach is only likely to further fuel mistrust between EU member states with significantly different criminal justice traditions and systems.

Also, by envisaging that the proposed orders could be issued directly by prosecutors for certain categories of information, the preservation of production of which can seriously interfere with fundamental rights, or in a potentially wide range of urgent cases, the Commission and Council proposals do not systematically allow for an adequate level of effective judicial protection in the country of issue.

9.3 Legal uncertainty

The proposed e-evidence rules have far-reaching negative implications for legal certainty.

EU law grants the right to an effective remedy to suspects and accused persons, as well as to concerned third parties whose rights might be affected by the execution of a data-gathering measure. Under the e-evidence proposal, however, the lack of (systematic and/or meaningful) involvement of the competent oversight authorities in the executing or affected states limits this right.

Without the opportunity to seek remedies in the executing state, the risk exists of an increase in the number of appeals made against companies through civil law, which do not qualify as effective remedies in criminal justice.

Important concerns have been raised by defence lawyers in relation to not only the guarantees of fair-trial rights, but also the need to preserve legal professional privilege/professional secrecy.

Companies face serious risks of liabilities simply for complying with foreign orders in good faith. Service providers should not be held liable for prejudice towards their users or third parties resulting exclusively from complying with an EPO or an EPO-PR in good faith. And yet, in the absence of a clear obligation for the judicial authorities in the executing country to formally review, validate and consequently authorise the data transfer to the country issuing the EPO, no legal certainty can be granted to service providers.

Several service providers are also concerned by the possibility of having to bear the costs associated with executing potentially high volumes of orders, while at the same time being obliged to seek reimbursement in a different country to the one where they are established or provide their services. Costs normally related to the correct functioning of criminal justice cooperation cannot be outsourced to private companies.

9.4 Police authorities' direct cooperation with foreign service providers

Direct cross-border cooperation between law enforcement authorities and service providers should not be allowed within the EU.

This type of cooperation does not qualify as judicial cooperation in criminal matters under EU law. At the same time, judicial cooperation guarantees provided through the EIO and the MLAs cannot simply be bypassed by framing cross-border access to data as a law-enforcement issue.

Under US law, US service providers can respond on a voluntary basis to foreign law-enforcement requests for data so far as they target non-content data pertaining to non-US

citizens or residents. Requests for non-content data are, in fact, currently received by the European subsidiaries of US internet or cloud service providers, which process them in line with their own internal guidelines.

And yet EU member states' law-enforcement authorities' practices of direct cooperation with US service providers cannot run contrary to – or fall short of – EU legal benchmarks. The same applies to direct cross-border law-enforcement requests for access to WHOIS data.

EU member states' national authorities are bound by EU law and cannot operate outside the EU legal framework. Nor can their external actions compromise the coherent application of the data protection and criminal justice *acquis*.

More information must be gathered on current direct public-private cooperation practices followed by EU member states, to assess whether they are effectively in line with EU data-protection legislation, including the GDPR and the Data Protection Directive.

In the meantime, the EU should support the role and capacities of national data-protection authorities (DPAs), which under EU law are entrusted with a crucial oversight role. DPAs should be adequately staffed and equipped with sufficient human and technical resources. Their independence and impartiality from EU member state governments should be preserved. This is an essential precondition for these bodies to qualify as effective remedies under EU privacy and data-protection laws.

It should also be verified whether EU member states effectively comply with provisions included in the Access to Information Directive, which specifies that the defence should have access to the file and, most notably, all essential materials to challenge detention.

10. GUARANTEEING EU STANDARDS IN TRANSATLANTIC AND INTERNATIONAL COOPERATION

The EU has the positive responsibility to promote and protect – through external action – its fundamental rights and rule of law standards abroad. It is also responsible for ensuring that third-country or multilateral cooperation initiatives do not compromise the coherent and effective application of the EU criminal justice and data protection *acquis*.

Conflicts of law and jurisdiction are unavoidable in the presence of unilateral assertions of criminal jurisdiction by authorities operating under different criminal systems and traditions. EU cooperation with third countries needs to rely strictly on instruments providing effective oversight mechanisms, with the ability to systematically verify – on a case-by-case basis – that EU fundamental rights' safeguards are fully complied with.

10.1 Investing in the MLAT system

Investment and innovation in EU MLA instruments is the way forward for EU criminal justice cooperation with the US and other third countries.

When cooperating with third countries in fields such as cross-border evidence gathering, the EU member states are now bound to comply with the EU criminal justice and data protection *acquis*, as dynamically interpreted by the CJEU. International transfers of data for law-enforcement and criminal justice purposes can only comply with EU law if based on instruments capable of effectively guaranteeing that third countries' data processing do not compromise EU fundamental rights protections.

By subjecting cross-border requests for data to mutual and systematic judicial scrutiny, MLA agreements give the competent judicial authorities of each of the parties concerned the possibility of effectively reviewing the measure issued.

The involvement of EU national courts is an especially important legal-certainty requirement, allowing EU courts and judges to scrutinise incoming requests from foreign authorities against EU legal standards. It also permits them to ask for the intervention of the CJEU if they believe a third-country request for data is in breach of EU fundamental rights, as enshrined in the Charter.

Digitalisation can help render the MLA process more effective. New EU investments in digital infrastructures for cross-border judicial cooperation can speed up the processing, validation and exchange of MLA requests. EU investments in this area could focus on digital certifications, and the secure transmission, intake and processing of MLA requests. New technologies can also help national authorities to easily access the information needed to formulate 'quality MLA

requests', to provide standardised electronic forms for their transmission, and to facilitate their tracking and follow up throughout different procedural stages.

The EU should develop programmes to build the technical knowledge of EU judicial authorities. It is necessary to improve EU authorities' ability to draft preservation and production requests that are up to the US standards. Low-quality requests still have to be processed, causing delays in the US and frustrations in the EU.

To increase consistency and foster legal certainty in cross-border data-gathering, the Commission (supported by Eurojust) should develop comprehensive guidelines. These should be based on existing promising practices, allowing transatlantic emergency requests to be issued and executed while relying on the EU-US MLA cooperation agreement and related oversight mechanisms.

A thorough and independent evaluation of the EU-US Umbrella Agreement implementation should be performed. More knowledge is needed to assess the impact and effectiveness of such an instrument in ensuring that personal data exchanged between the EU and the US are protected in line with EU data-protection requirements. It should be exactly verified what type of remedies are currently available to EU citizens under the US Judicial Redress Act, and whether such remedies meet the necessary EU legal and judicial-protection standards.

The EU should not engage in international or transatlantic negotiations aimed at introducing instruments that would grant third countries – who are governed by different criminal justice and data-protection standards – the potential to directly access data held by service providers under EU jurisdiction.

This type of data-gathering practice does not qualify as a form of judicial cooperation within the EU criminal justice area, and *a fortiori* it should not be allowed in cooperation with third countries. Unlike within the EU, cooperation with third countries is not built on shared values and fundamental principles, the harmonisation of laws and procedural guarantees, or mechanisms for cooperation and supervision.

10.2 Preserving the coherence of EU *acquis* through external action

The Lisbon Treaty introduces a duty to uphold and promote EU values in the Union's external actions. When negotiating a transatlantic agreement, an agreement with the UK, or the CoE protocol, the EU has an obligation to fully comply with its internal *acquis*. This does not include secondary law as interpreted by the CJEU (in fields such as mutual recognition in criminal matters and data-protection law) nor, of course, the EU Charter.

There is a proliferation of initiatives promoting new international tools of direct public-private cooperation for data gathering for law enforcement purposes. This poses crucial coherency and legal certainty challenges, from an EU criminal justice and data-protection perspective.

Pieces of foreign legislation such as the CLOUD Act (Part I and II), or international cooperation initiatives such as the Second Additional Protocol to the Budapest Convention, may affect

common EU rules or alter their scope. This can occur when the areas covered overlap with EU legislation or are covered to a large extent by EU law.

International initiatives, such as the US-UK Agreement under the CLOUD Act, risk compromising the effective protection of EU data-protection and criminal-justice standards. An in-depth examination of the content, functioning and implications of such agreements must be included by the Commission when conducting its adequacy assessment of the UK and US data-protection *acquis*.

No adequacy decisions should be adopted on finding that these third countries do not ensure an adequate level of protection of human rights, nor provide for appropriate safeguards. In the absence of an adequacy decision, transfers of personal data may only take place based on the procedures and mechanisms provided by a legally binding instrument (i.e. an MLA agreement) that provides appropriate safeguards to protect personal data. As clearly established by the EU Data Protection Directive, in the absence of both an adequacy decision and appropriate safeguards, personal data can be transferred only in exceptional circumstances and on a case-by-case basis.

Effective judicial oversight over incoming data requests is especially important in preventing foreign requests for data from compromising the essence of EU fundamental rights *acquis*. The importance of such oversight has been recently restated by the CJEU. It found not only that US surveillance statutes and related laws do not meet basic proportionality requirements, but also that non-US persons do not have access to any meaningful remedy before US courts.

With negotiations on the Second Additional Protocol to the Budapest Conventions moving ahead, EU participation in this international rule-making forum should aim strictly at ensuring that the integrity of the existing EU *acquis* is preserved. The proposed e-evidence rules should not be taken as a reference point for the development of EU external actions or positions.

The Commission should ensure that the negotiations of the Protocol do not lead to the adoption of instruments (e.g. international production orders) that would allow third countries or member states' authorities to access data subject to EU jurisdiction, outside existing EU instruments of judicial cooperation. The objective of equipping law-enforcement authorities with new tools for fighting cybercrime should not justify the introduction of instruments that are incompatible with EU law.

Any new instruments for cross-border data gathering should include mechanisms for systematic ex ante review of foreign measures by judicial authorities in the country of execution. These instruments should include clear grounds of refusal in the absence of double criminality, or when it turns out that the requested data are covered by professional secrecy or legal privilege.

The Commission should also ensure that definitions of data covered by the Protocol are consistent with the data categorisation adopted by existing EU legal instruments.

Disconnection clauses should be included in the Protocol, providing that member states continue, in their mutual relations, to apply EU rules rather than the Protocol's. EU law should

take precedence over the Second Additional Protocol. Furthermore, safeguards in the Second Additional Protocol should be higher than the ones applying for intra-EU cooperation.

Regardless of the powers entrusted to investigating and prosecuting authorities (as well as the authorities of other state parties) by international cooperation instruments, the principles, rules, conditions and safeguards currently enshrined in EU criminal justice and data-protection law should be complied with by EU member states.

REFERENCES

Abraha H.H. (2019), "How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis", 9 International Data Privacy Law 207.

Article 29 Working Party (2013), *Comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime*, 05 December 2013.

Bignami, F. (2015), *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, May 15, 2015.

Brodowski, D. (2020), "European Criminal Justice – From Mutual Recognition to Coherence", in Carrera, S., Curtin, D., Geddes, A. (Eds.), 20 Year Anniversary of the Tampere Programme: Europeanisation Dynamics of the EU Area of Freedom, Security and Justice European University Institute, 2020.

Brouwer, E. (2017), *International Cooperation and the exchange of personal data*, in Carrera and Mitsilegas (2017), 'Constitutionalising the Security Union: Effectiveness, rule of law and rights in countering terrorism and crime', CEPS Paperback.

Carrera, S., González Fuster, Guild, Mitsilegas, (2015), *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to the Rule of Law and Fundamental Rights*, CEPS Paperback Series.

Carrera, S., Mitsilegas, Stefan, Giuffrida, (2018), *The Future of EU-UK Criminal Justice and Police Cooperation, Towards a Principled and Trust-Based Partnership*, CEPS Task Force Report.

Carrera S., and Stefan, M. (2020), *Access to Data for Criminal Investigation Purposes in the EU*, CEPS Paper in Liberty and Security in Europe No. 2020-01, February 2020.

CCBE (2019), *Comments Draft 2nd Additional Protocol to the Convention on Cybercrime Provisional draft text of provisions (1 October 2019) on Language of requests, Emergency MLA, Video conferencing, direct disclosure of subscriber information, and giving effect to orders from another Party for expedited production of data*, 8 November 2019.

Daskal, J. and Swire, P. (2019), *The UK-US CLOUD Act Agreement Is Finally Here, Containing New Safeguards,* Just Security.

EDPB (2018), *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25 May 2018.

EDPB (2019), *Contribution to the consultation on a draft second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)*, 13 November 2019.

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.

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

EuroISPA (2019), *EuroISPA's comments on the provisional text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime.*

Fair Trials (2020), *Beyond the emergency of the COVID-19 pandemic: lessons for defence rights in Europe*, 20 July 2020.

González Fuster, G., and Vázquez Maymir, S. (2020*), Cross-border Access to E-Evidence: Framing the Evidence*, CEPS Paper in Liberty and Security, No. 2020-02, February 2020.

Guerra, J.E. and Janssens, C. (2018), *Legal and Practical Challenges in the Application of the European Investigation Order Summary of the Eurojust Meeting of 19–20 September 2018*, Eucrim, 2019/1.

Kuner, C. (2020), *The Schrems II judgment of the Court of Justice and the future of data transfer regulation*, European Law Blog, 17 July 2020.

Lenaerts, K., 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal.

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

Mitsilegas, V. (2020), *Responding to Covid-19: Surveillance, Trust and the Rule of Law*, 26 May 2020.

Mitsilegas (2017), "The Security Union as a paradigm of preventive justice: Challenges for citizenship, fundamental rights and the rule of law", in S. Carrera and V. Mitsilegas (Eds.), Constitutionalising he Security Union: Effectiveness, rule of law and rights in countering crime and terrorism, CEPS Paperback.

Mitsilegas, V. (2015), "Judicial Concepts of Trust in Europe's Multi-Level Security Governance: From Melloni to Schrems via opinion 2/13", Eucrim, Issue 3/2015.

Rojszczak, M. (2020), "CLOUD act agreements from an EU perspective", Computer Law & Security Review, Volume 38, September 2020.

Rotenberg, M. (2020), "Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection", European Law Journal 2020, 1.

Stefan, M. and González Fuster (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 Research Paper No. 2018-07, November 2018 (updated in May 2019).

Swire, P. (2019), *When does the GDPR Act as a Blocking Statute? The relevance of a Lawful Basis for Transfer*, Cross-Border Data Forum, November 2019

Wexler, R. (2019), "Privacy Asymmetries: Access to Data in Criminal Investigations", UCLA Law Review, Vol. 68, No. 1, 2021.

ANNEX I. LIST OF MEMBERS

Laure Baudrihaye-Gerard
Senior lawyer, Fair Trials Europe

Fabrizia Bemer
Office of the Public Prosecutor, Ministry of Justice, Italy

Ralf Bendrath
Adviser on Civil Liberties, Justice and Home Affairs, The Greens, European Parliament

Martin Böse
Chair for Criminal Law and Procedure, International and European Criminal Law, Rheinische Friedrich-Wilhelms-Universität

Dominik Brodowski
Junior Professor for Criminal Law and Criminal Procedure, Saarland University

Tony Bunyan
Investigative journalist specialising in justice and home affairs, civil liberties and freedom of information in the EU, Director Emeritus of Statewatch

Sara Bussière
Senior European Advisor, Orange

Sergio Carrera
Senior Research Fellow & Head of JHA Unit, CEPS

Simone Cuomo
Senior Legal Advisor, Council of Bars and Law Societies of Europe

Emilio De Capitani
Visiting Professor at Queen Mary's Law School (London)

Roland Doll
Vice President European Affairs, Deutsche Telekom

Anand Doobay
Lawyer, Boutique Law LLP

Michele Dubrocard
Administrator, European Parliament

Philip Eder
Senior Manager Government Affairs EMEIA – Apple

Anze Erbeznik
Administrator, European Parliament

Gloria Gonzalez Fuster
Research Professor, VUB

Paolo Grassia
Director of Public Policy, ETNO – European Telecommunications Network Operators

Caroline Greer
Head of European Public Policy, Cloudflare

Andreas Gruber
Legal Officer, EuroISPA

Sandra Karlsson
EU Public Policy Program Manager, Amazon Web Services Public Policy

Katalin Ligeti
Professor of European and International Criminal Law, University of Luxembourg

Claire-Agnès Marnier
Legal Officer, EDPS – European Data Protection Supervisor

Holger Matt
Lawyer, Rechtsanwaltskanzlei Prof. Dr. Holger Matt

Claire-Agnès Marnier
Legal Officer, EDPS – European Data Protection Supervisor

Iain Mitchell
Lawyer/Council of Bars and Law Societies of Europe

Valsamis Mitsilegas
Professor of European Criminal Law and Global Security and Deputy Dean for Global Engagement (Europe), Queen Mary University of London

Katherina Neuffer
Counsellor, Justice and Consumer Policy, Permanent Representation of the Federal Republic of Germany to the European Union

Harvey Palmer
Deputy Head of Policy, Crown Prosecution Service

Jan Penfrat
Senior Policy Advisor, EDRI

Erik Planken
Senior Policy Advisor Cybercrime, Ministry of Justice & Security, The Netherlands

Elena Plexida
Government and IGOs Engagement Sr Director, ICANN

Sebastian Raible
Policy Advisor / Parliamentary Assistant to MEP Sergey Lagodinsky, European Parliament

Juraj Sajfert
Scientific Researcher, Vrije Universiteit Brussel

Maximilian Schubert
President, EuroISPA

Niksa Stolic
Legal Officer, EDPS – European Data Protection Supervisor

Kazimierz Ujazdowski
Legal Officer, Supervision and Enforcement Unit, EDPS – European Data Protection Supervisor

Nick Vamos
Partner, Peters & Peters, Former Head of Special Crime and Head of Extradition at the Crown Prosecution Service

Catherine Van de Heyning
Professor European Fundamental Rights Law, University of Antwerp

Wouter van Ballegooij
Policy Analyst, European Parliamentary Research Service

Cristina Vela
The Data Protection, Trust & Security (DPTS) WG Chair, ETNO, Telefonica

Caroline Walczak
European Affairs Advisor, Orange

Rebecca Wexler
Assistant Professor of Law, the University of California, School of Law

Caroline Wilson Palow
Legal Director and General Counsel, Privacy International

ANNEX II. TASK FORCE MEETINGS AGENDAS

Task Force on

Cross-border data in the fight against crime

What future for e-evidence?

Kick off Meeting

Brussels, 23 January 2020
CEPS, Place du Congrès 1, 1000, Brussels
9:00am to 12:30 pm

Agenda

9:00 9:30	**Registration**	
9:30 10:00	Welcoming words & introduction to the Task Force	• Sergio Carrera Senior Research Fellow and Head of the Justice and Home Affairs Section, CEPS • Valsamis Mitsilegas Professor of European Criminal Law and Global Security and Deputy Dean for Global Engagement (Europe), QMUL • Marco Stefan Research Fellow, Justice and Home Affairs section, CEPS
	Panel Discussion	
10:00 10:45	Chair Sergio Carrera	**Speakers** • Lani Cossette Director EU Affairs, Microsoft • Cristina Vela Chair of Data Protection, Trust & Security Working Group, ETNO • Caroline Greer Head of European Public Policy, Cloudflare • Maximilian Schubert Secretary General, EuroIspa **Discussants** • Catherine Van De Heyning Assistant Professor European Fundamental Rights Law, University of Antwerp • Juraj Sajfert Research Fellow, Vrije Universiteit Brussel • Simone Cuomo Senior Legal Advisor, Council of Bars and Law Societies of Europe
10:45 12.30	**Round table discussion**	• All Task Force Members

Task Force on

Cross-border data in the fight against crime

What future for e-evidence?

First Task Force Meeting

Towards a new E-evidence regulation: what legal and practical challenges ahead?

Brussels, 10 March 2020
CEPS, Place du Congrès 1, 1000, Brussels
9:00am to 12:00 pm

Agenda

9:00 9:30	**Registration**	
9:30 9:45	Welcoming words & introduction	• Sergio Carrera Senior Research Fellow and Head of the Justice and Home Affairs Section, CEPS • Marco Stefan Research Fellow, Justice and Home Affairs section, CEPS
	Panel Discussion	
9:45 11:00	Chair Valsamis Mitsilegas	**Speakers** • Isabelle Pérignon Deputy Head of Cabinet of Didier Reynders, EU Commissioner for Consumer and Justice • Erik Planken Senior Policy Advisor Cybercrime, Ministry of Justice & Security, The Netherlands (Remotely) • Anze Erbeznik Policy Administrator, LIBE Secretariat, European Parliament **Discussants** • Fabrizia Bemer Office of the Public Prosecutor in Florence, Ministry of Justice, Italy (Remotely) • Iain Mitchell QC, Council of Bars and Law Societies of Europe
11:45 12.00	**Round table discussion**	• All Task Force Members

Task Force on

Cross-border data in the fight against crime

What future for e-evidence?

Second Task Force Meeting (Webinar)

COVID-19 Implications on EU judicial cooperation

Digitalisation and the role of data in cross-border evidence-gathering

---

Brussels, 30 April 2020
9:00am to 10:30 pm

Agenda

9:00 9:30	**Registration**	
9:30 10:00	Welcoming words & introduction	• Sergio Carrera Senior Research Fellow and Head of the Justice and Home Affairs Section, CEPS
	Panel Discussion	
10:00 10:45	Chair Marco Stefan Research Fellow, Justice and Home Affairs section, CEPS	**Speakers** • Sergey Lagodinky Member of the LIBE Committee, European Parliament • Cristian Nicolau Head of Unit B4 – eJustice, IT, Logistics and Document Management, DG Consumers and Justice, European Commission • Fabrizia Bemer Office of the Public Prosecutor in Florence, Italian Ministry of Justice **Discussants** • Laure Baudrihaye-Gérard Senior Lawyer, Fair Trials Europe • Caroline Wilson Palow Director, Privacy International
10:45 12.30	**Round table discussion**	• All Task Force Members
	Closing Remarks	• Valsamis Mitsilegas Professor of European Criminal Law and Global Security and Deputy Dean for Global Engagement (Europe), QMUL

Task Force on

Cross-border data in the fight against crime

What future for e-evidence?

International cooperation for data gathering in criminal investigations and the external components of the E-Evidence Package

Third Task Force Meeting (Webinar)

Brussels, 03 June 2020
15:00pm to 17:00 pm

Agenda

15:00 15:05	Welcoming words & introduction	• Sergio Carrera Senior Research Fellow and Head of the Justice and Home Affairs Unit, CEPS
	Panel Discussion	
15:05 16:15	Chair Marco Stefan Research Fellow, CEPS Justice and Home Affairs Unit	**Speakers** • Kenneth Harris Senior Counsel for EU and International Criminal Matters U.S. Department of Justice U.S. Mission to the EU • Harvey Palmer Deputy Director Policy, Strategy and Policy Directorate, Crown Prosecution Service **Discussants** • Anna Buchta Head of Policy and Consultations Unit, European Data Protection Supervisor • Rebecca Wexler, Assistant Professor of Law, UC Berkley School of Law • Sabine Gless Professor of Criminal Law and Criminal Procedural Law, University of Basel, Switzerland
16:15 16:55	Q/A Session	• All Task Force Members
16:55 17:00	Closing remarks & Next steps	• Valsamis Mitsilegas Professor of European Criminal Law and Global Security, QMUL • Sergio Carrera Senior Research Fellow and Head of the Justice and Home Affairs Unit, CEPS

Providers of internet, cloud and electronic communication services hold information that is sought and used extensively for detecting, preventing, investigating and prosecuting various types of crime, regardless of whether they are committed through the internet or in the offline world. Yet increasing demands for data in criminal proceedings do not automatically justify foregoing the system of mutual judicial checks and guarantees that currently govern intra-EU and international cooperation for cross-border evidence gathering in criminal matters. In fact, the widespread use of information and communication technologies increasingly exposes people's rights and freedoms to investigative and prosecuting state machineries. Ensuring systematic and effective judicial oversight of cross-border data requests becomes especially important when such measures originate from a wide range of authorities operating within different criminal justice systems, with different criminal justice traditions.

This book takes stock of the EU constitutional principles and legal instruments relating to internal and external criminal justice cooperation in the field of data gathering. It examines the issues of legal uncertainty raised by EU, US and international initiatives directed at promoting different forms of direct public-private cooperation on cross-border data access in criminal proceedings.

The authors present the result of discussions between members of a Task Force set up jointly by CEPS and the Global Policy Institute at Queen Mary University of London. Based on the insights of the Task Force, they identify solutions to facilitate judicial cooperation in cross-border gathering of data, without jeopardising the rule of law and EU citizens' fundamental rights.

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C008551

9 789461 387806

Queen Mary University of London

CENTRE FOR EUROPEAN POLICY STUDIES
CEPS