The push for the international regulation of cross-border access to electronic evidence and human rights

El impulso para la regulación internacional del acceso transfronterizo a las pruebas electrónicas y los derechos humanos

Ana Gascón Marcén*
Profesora Contratada Doctora de Derecho Internacional Público
Universidad de Zaragoza

Recibido:13.12.2022/Aceptado:24.01.2022
DOI: 10.20318/cdt.2023.7545

Abstract: This paper describes the different solutions used by China, the United States and the European Union to access electronic evidence for criminal investigations and the problems raised by their different approaches. The unstoppable trend to create mechanisms that allow authorities from one State to request data directly from a service provider located in another State is assessed together with the human rights challenges it poses and the need for the inclusion of certain safeguards in this kind of initiatives. The Second Protocol to the Budapest Convention is also analyzed as a recently negotiated multilateral solution to tackle this issue.
Keywords: CLOUD Act, cross-border access, electronic evidence, Budapest Convention.

Resumen: Este artículo describe las diferentes soluciones utilizadas por China, Estados Unidos y la Unión Europea para acceder a pruebas electrónicas para investigaciones penales y los problemas que plantean sus diferentes enfoques. Se evalúa la tendencia imparable de crear mecanismos que permitan a las autoridades de un Estado solicitar datos directamente a un proveedor de servicios ubicado en otro Estado, los desafíos en materia de derechos humanos que plantea y la necesidad de incluir ciertas salvaguardas en este tipo de iniciativas. También se analiza el Segundo Protocolo del Convenio de Budapest como una solución multilateral negociada recientemente para abordar este problema.
Palabras clave: CLOUD Act, acceso transfronterizo, pruebas electrónicas, Convenio de Budapest

* Senior lecturer at the Faculty of Law of the University of Zaragoza. Member of the research team of the project "Towards a person-centred digital transition in the European Union" (TRADIPER). This publication is part of the TED2021-129307A-I00 project, funded by MCIN/EIP/10.13039/501100011033 and the European Union's "NextGenerationEU"/PRTR.

I. Introduction

1. Access to electronic evidence has become a key element in police investigations, not only when it comes to prosecuting cybercrime, but any kind of crime. According to the European Commission, electronic evidence in any of its forms is relevant in about 85% of criminal investigations and, in almost two thirds (65%) of those, the service providers to whom the requests are directed are located in a different jurisdiction. The combination of the two previous percentages results in 55% of the total investigations in the European Union (EU) including a request for cross-border access to electronic evidence.[1]

2. The first problem in obtaining and securing electronic evidence is the nature of the Internet itself. It poses serious challenges as jurisdiction is usually linked to the territory of the State, but the Internet has no borders. The intermediary that has the information may not be established in the same country where the criminal investigation is being carried out or, even if it is the case, the data may be on servers abroad. This may happen even in domestic investigations when the victims and perpetrators are all located in the same country where the investigation is taking place, but the data may be elsewhere. The characteristics of electronic evidence add more problems as data are stored, duplicated or moved between servers somewhere in the cloud, in possibly multiple or unknown jurisdictions, which also makes them tremendously volatile.[2]

3. There are instruments at the international level to facilitate access to evidence located in other jurisdictions, such as MLA mechanisms, but the requests may take quite a lot of time to be answered, on average between six and twenty-four months.[3] Therefore, many investigations are abandoned and closed without results.

4. In this paper, we describe the different solutions used by the main actors in the field and its problems (section II), in particular, the mechanisms created by China (subsection 1), the United States (subsection 2) and the EU (subsection 3). In addition, the multilateral solution presented by the Second Protocol to the Budapest Convention is analyzed (section III), to finish with some brief conclusions (section IV).

II. Different unilateral solutions to facilitate access to electronic evidence

5. In this section, we study the solutions to this problem put in practice by China, the United States, and the EU. China and the United States are the two most powerful countries in the world in geostrategic terms. On top of that, they host the largest digital companies by market cap.[4] In the case of the United States, those are Apple, Microsoft, Amazon, Alphabet (Google) or Meta (Facebook), and, for China, Tencent and Alibaba, but there are many more. These tech giants control a huge share of the digital data of the world.

---

[1] European Commission, *Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD/2018/118 final – 2018/0108 (COD), 17 April 2018, 14.

However, Vazquez Maymir challenges the empirical soundness of these findings and argues that the percentages and figures used frame the problem fundamentally on technical and efficiency grounds, while there is no reference to the political and economic motivations behind the promotion of a policy shift from mutual legal assistance (MLA) treaties to direct cooperation, which, in his view, is the fourth and lost premise. See S. Vazquez Maymir, "Anchoring the need to revise cross-border access to e-evidence", *Internet Policy Review,* vol. 9, nº 3, 2020 <https://doi.org/10.14763/2020.3.1495> accessed 13 December 2022.

[2] J. Kleijssen and P. Perri, "Cybercrime, Evidence and Territoriality: Issues and Options", *Netherlands Yearbook of International Law,* 2017, pp. 147-173, p. 150 <https://rm.coe.int/cybercrime-evidence-andterritoriality-issues-and-op-tions/168077fa98> accessed 13 December 2022.

[3] T-CY, *The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, TCY(2013)17rev, Council of Europe, 2014, p. 123.

[4] See <https://companiesmarketcap.com/> accessed 2 December 2022.

6. The case of the EU and its cooperation mechanism to solve this problem is also studied because it is the agreed solution for its 27 Member States and, in addition, it could have a significant impact outside of the frontiers of the EU, as its GDPR[5] is a golden standard in the field of data protection[6] and its digital solutions are copied in different jurisdictions and applied by some companies at a global level.[7] This is known as the Brussels's effect.[8] Some authors have also theorized that there may be another trend of influence coming from China in the digital realm baptized as the Beijing's effect.[9]

1. China and Data Localization

7. China is the most famous example of a country with a strict data localization policy, but other States follow it to different degrees such as Russia,[10] India, Indonesia or Vietnam[11]. Cory and Dascoli describe China as the most data-restrictive country in the world, followed by Indonesia, Russia and South Africa.[12]

8. A good deal of the data collected or generated in China must be stored in its territory according to its Cybersecurity Law, Data Security Law and Personal Information Protection Law.[13] This is coupled with the prohibition of some data overseas transfers. The Data Security Law expressly prohibits providing any data stored in China to law enforcement authorities or judicial bodies outside of China without prior Chinese government approval.

9. Data localization is highly effective as it gives Chinese public authorities unfettered access to the data. Abraha argues that, from the perspective of law enforcement access, data localization policies are perceived to serve a dual purpose: 'facilitative' and 'preventive'.[14] They enable the law enforcement authorities within the imposing country or region to access data using domestic procedures and, at the same time, prevent foreign governments from having such straightforward access.

---

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJEU L 119, 4 May 2016, p. 1.

[6] See G. Buttarelli, "The EU GDPR as a Clarion Call for a New Global Digital Gold Standard", *International Data Privacy Law,* vol. 6, nº 2, 2016, pp. 77-78 and A. Mantelero, "The future of data protection: Gold standard vs. global standard" *Computer Law & Security Review*, vol. 40, 2021 <https://doi.org/10.1016/j.clsr.2020.105500> accessed 13 December 2022.

[7] G. Greenleaf and B. Cottier, "2020 Ends a Decade of 62 New Data Privacy Laws", *Privacy Laws & Business International Report,* nº 163, 2020.

[8] A. Bradford, *The Brussels Effect. How the European Union rules the world,* Oxford University Press, 2020.

[9] M. S. Erie and T. Streinz, "The Beijing effect: China's "digital silk road" as transnational data governance", *New York University Journal of International Law and Politics,* Vol. 54, 2021.

[10] See A. Savelyev, "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?", *Computer Law & Security Review,* vol. 32, no. 1, 2016 <https://www.sciencedirect.com/science/article/pii/S0267364915001685> accessed 13 December 2022.

[11] Even if Indonesia and Vietnam had loosened some of their data retentions restrictions, see A. Basu, "The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam", *The Diplomat,* 10 January 2020 <https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/> accessed 13 December 2022.

[12] N. Cory and L. Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, Information Technology & Innovation Foundation, July 2021 <https://www2.itif.org/2021-data-localization.pdf> accessed 13 December 2022.

[13] For a more detailed description of the data localisation regime, see Y. Luo, Z. Yu and V. Liu, "The future of data localization and cross-border transfer in China: a unified framework or a patchwork of requirements?", *IAPP,* 22 June 2021 <https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements/> accessed 13 December 2022.

Data localization mainly applies to "personal information" and "important data" in the hands of critical information infrastructure operators, but there are also requirements in sectoral laws for example dealing with automotive operators.

[14] H. H. Abraha, "Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives", *International Journal of Law and Information Technology,* Vol. 29, no. 2, Summer 2021, pp. 118–153, p. 130 <https://doi.org/10.1093/ijlit/eaab001> accessed 13 December 2022.

10. China's data localization has been extremely criticized from several perspectives. It is a building block of China's Social Credit System, which according to Greenleaf is emerging as the world's most pervasive and potentially totalitarian surveillance system[15] and it is often cited as an example of how data localization can be used for political repression.[16]

11. Access Now considers that data localization in China threatens human rights while at the same time it is highly questionable its value for cybersecurity.[17] In general, Freedom House argues that domestic data storage requirements place users' data firmly in the legal purview of governments, significantly enhancing authorities' surveillance capabilities by lowering access barriers to data. It highlights the risks for privacy, freedom of expression, access to information, press freedom, freedom of belief, non-discrimination, freedom of assembly and association and due process.[18]

12. Data localization also poses problems from an e-commerce perspective as it fragments markets.[19] The EU and the US have criticised it in the framework of the WTO[20]. The US considers it as a trade barrier.[21] Some authors question how China could join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) as it is its intention, considering that this free trade agreement strongly promotes free cross-border data flows by strictly prohibiting the data localization requirement, setting a relatively high threshold for government interventions to meet public policy objectives by applying the WTO type general exception clauses.[22] In addition, Cory and Dascoli argue that restricting data flows has a statistically significant impact on a nation's economy—sharply reducing its total volume of trade, lowering its productivity, and increasing prices for downstream industries that increasingly rely on data.[23]

2. The United States and the CLOUD Act

13. The US opted for quite a different solution. It passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act in 2018. This legislative development was motivated by a case where Microsoft refused to comply with a US court warrant requesting the content of emails stored on a server in Ireland as part of a drug investigation that was taking place in the US. The case reached the Supreme Court (*United States of America v. Microsoft Corporation*).[24] However, before the case was decided the CLOUD Act was passed rending it moot.

---

[15] G. Greenleaf, "Asia's Data Privacy Dilemmas 2014–19: National Divergences, Cross-Border Gridlock", *Revista Uruguaya de Protección de Datos Personales,* vol. 4, 2019, pp. 49-73, p. 54.

[16] D. Svantesson, *Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines*, OECD Digital Economy Papers, No. 301, OECD Publishing, Paris, 2020.

[17] Access Now, "A closer look at China's Cybersecurity Law — cybersecurity, or something else?" (13 December 2017) <www.accessnow.org/closer-look-chinas-cybersecurity-law-cybersecuritysomething-else/> accessed 13 December 2022.

[18] A. Shahbaz, A. Funk and A. Hackl, *User privacy or cyber sovereignty? Assessing the human rights implications of data localization,* Freedom House, 2020 <https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty> accessed 13 December 2022.

[19] D. Svantesson, *op. cit.*

[20] *Joint Statement on Electronic Commerce. EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce. Communication from the European Union*, 26 April 2019 <https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf> accessed 13 December 2022 and *Joint Statement on Electronic Commerce. Communication from the United States*, 26 April 2019 (leaked document).

[21] See United States Trade Representative, *2022 National Trade Estimate Report on Foreign Trade Barriers*, 2022 <https://ustr.gov/sites/default/files/2022%20National%20Trade%20Estimate%20Report%20on%20Foreign%20Trade%20Barriers.pdf> accessed 13 December 2022.

[22] M. Morita-Jaeger and G. Larbalestier, "The economics and politics of China's accession to the CPTPP", *UK Trade Policy Observatory,* 7 October 2021 <https://blogs.sussex.ac.uk/uktpo/2021/10/07/chinas-accession-to-the-cptpp/> accessed 13 December 2022. The authors consider that the CPTPP approach is completely different to China's state-led digital governance, which has a strong notion of data sovereignty with China strengthening its authoritarian power in laws on data over the last several years.

[23] N. Cory and L. Dascoli, *op. Cit.*

[24] For an in-depth study of the challenges presented by this case, A. J. Colangelo and A. L. Parrish, *International Law and Extraterritoriality: Brief of International and Extraterritorial Law Scholars as Amici Curiae (U.S. v. Microsoft),* SMU Dedman School of Law Legal Studies Research Paper No. 382, 2018.

14. The first part of this federal law states that a provider of electronic communication service or remote computing service under US jurisdiction shall preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether it is located within or outside of the US. Thus, US authorities through a subpoena or warrant can compel Internet intermediaries to handle data even if it is stored abroad.

15. This is quite a useful solution for a country like the US because of the high number of relevant technological companies based in its territory. However, it will not be well suited for other countries where it would be way less effective as they would want to get data from intermediaries located elsewhere. In addition, this can create friction with the contradicting obligations for example if an American company must produce data against what is stated in the GDPR.[25]

16. Further conflict with the US may be caused because the *Stored Communications Act* contains a blocking statute that forbids US providers to facilitate content data to a foreign authority if there is not an agreement between that State and the US. This will make it impossible for US-based intermediaries to comply in some cases with the future European production and preservation orders, explained *infra*. This is problematic because many of the data requests from the EU go to providers based in the US.

17. The second part of the CLOUD Act provides an expedited route to MLA treaties through executive agreements. The executive branch can enter into bilateral agreements with foreign countries to provide requested data related to its citizens in a streamlined manner. The first agreement of this kind was signed between the US and the UK. This Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime[26] enables law enforcement authorities in either country to request and obtain electronic communications content data directly from service providers located in the other country without having to collaborate with the authorities of that State and, thus, avoiding the long procedure of MLA mechanisms.

18. The agreement between the US and the UK has a legitimate purpose and advantages such as regulating some practices that were already being carried out through informal channels. However, its evaluation is ambivalent. It has been considered a clear breakthrough by some[27] or a step back by others,[28] and its lack of reciprocity has also been criticised[29].

---

[25] See *Joint letter of the EDPB and the EDPS addressed to Juan Fernando López Aguilar, Chair of the LIBE Committee on 10 July 2019*. <https://edps.europa.eu/sites/edp/files/publication/19-07-10_edpb_edps_cloudact_coverletter_en.pdf> accessed 13 December 2022. See T. Christakis, 'Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?' in R. Milch, S. Benthall and A. Potcovaru (eds), *Cybersecurity and Privacy in a Globalized World - Building Common Approaches*, New York University School of Law, e-book, 2019, pp. 60–76 <https://ssrn.com/abstract=3397047> accessed 13 December 2022; and J. Shurson, "Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law", *International Journal of Law and Information Technology,* Vol. 28, no. 2, Summer 2020, pp. 167–184.

[26] *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*. <www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019> accessed 13 December 2022.

[27] J. Daskal and P. Swire, 'The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards', *Lawfare*, 8 October 2019 <www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards> accessed 13 December 2022.

[28] K. Rodriguez and C. Fischer, 'A Race to the Bottom of Privacy Protection: The US-UK Deal Would Trample Cross Border Privacy Safeguards', *Electronic Frontier Foundation,* 4 October 2019 <www.eff.org/deeplinks/2019/10/race-bottom-privacy-protection-us-uk-deal-would-trample-cross-border-privacy> accessed 13 December 2022.

[29] See E. Mignon, 'The CLOUD Act: Unveiling European Powerlessness', *Revue européenne du droit,* vol. 1, 2020, pp. 108-116 <https://legrandcontinent.eu/fr/2020/09/05/the-cloud-act-unveiling-european-powerlessness/> and M. Rojszczak, 'CLOUD act agreements from an EU perspective', *Computer Law & Security Review,* Vol. 38, 2020 <"http://www.sciencedirect.com/science/article/pii/S0267364920300479#sec0005"www.sciencedirect.com/science/article/pii/S0267364920300479#sec0005> both accessed 23 December 2022.

19. The European Commission is currently negotiating an agreement with the US.[30] Some of the safeguards included in the Council mandate are: to ensure that data may not be requested for the use in criminal proceedings that could lead to the death penalty; to ensure necessity and proportionality of orders for access to electronic evidence, distinguishing in particular between data categories as appropriate; procedural safeguards for individuals subject to a data order in the framework of criminal proceedings; specific safeguards for data protected by privileges and immunities; and the confidentiality safeguards for authorities and service providers, including non-disclosure requirements.

20. The European Data Protection Supervisor (EDPS) recommended essential improvements and the reinforcement of several safeguards, notably the involvement of judicial authorities designated by the other Party to the agreement as early as possible in the process of gathering electronic evidence so that these authorities would have the possibility to review compliance of the orders with fundamental rights and raise grounds for refusal.[31]

21. In addition, there are some strong divergences between the EU and the US about what the scope and the architecture of this agreement should be. The US supports the conclusion of a framework agreement with the EU to be followed by bilateral agreements with Member States. While the EU wishes to arrive at a self-standing EU-wide comprehensive agreement and is opposed to solutions that might lead to fragmentation and unequal treatment between Member States.[32]

22. Abraha argues that the new generation of agreements envisioned by the CLOUD Act could serve as a starting point toward a cooperative future, and the envisaged EU–US agreement would be a breakthrough in addressing the cross-border data access problem. However, the negotiation will be a delicate task that requires grappling with complex policy issues and compromising on long-standing differences around privacy and security.[33]

23. As the agreement with the UK was the first to be finalized it can be considered as a blueprint for the future ones. It contains fewer safeguards regarding the protection of fundamental rights than those required by the EU mandate so the negotiations should be closely followed.[34]

3. The European Union and the European Production and Preservation Orders

24. The European Commission proposed the creation of two new co-operation mechanisms[35]:

[30] See Council Decision of 6 June 2019 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.

[31] See EDPS, *Opinion 2/2019 on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence*.

[32] See T. Christakis and F. Terpan, 'EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options', *International Data Privacy Law*, 2021 <https://doi.org/10.1093/idpl/ipaa022> accessed 13 December 2022.

[33] H.H. Abraha, op. Cit., p. 151.

[34] T. Christakis, '21 Thoughts and Questions about the UK/US CLOUD Act Agreement: (and an Explanation of How it Works – With Charts)', *European Law Blog*, 13 October 2019 <https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/> accessed 13 December 2022.

[35] Gómez Amigo finds paradoxical that the Commission Proposal characterizes the orders as instruments of mutual recognition in the field of criminal judicial cooperation, but it articulates a system, not of direct communication between judicial authorities, but between a judicial authority and a service provider, which is a private entity. Even if the author welcomes the Proposal, he finds concerning that the judicial control in the executing State will not happen in most cases, in a matter that fully affects personal data and privacy and, therefore, fundamental rights. See L. Gómez Amigo, "Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima". *Revista Española de Derecho Europeo*, vol. 71, 2019, pp. 23-56. In the same vein, Laro González cloncludes that we are once again witnessing the debate on whether security or greater protection of procedural rights and guarantees should prevail. See M. E. Laro González, "Prueba penal

the European Production and Preservation Orders for electronic evidence in criminal matters.[36] The European Production Orders (EPO) are binding decisions to produce electronic evidence, while the European Preservation Orders (EPO-PR) serve to preserve electronic evidence in view of a subsequent request for production. These last ones will be used to prevent the removal, deletion or alteration of relevant data in situations where it may take more time to obtain the production of this data, for example, because of the recourse to judicial cooperation channels.

25. The Regulation distinguishes four categories of data: subscriber data, access data, transactional data and content data. The Court of Justice of the EU(CJEU) has already stated that metadata of communications may allow very precise conclusions to be drawn concerning the private lives of people, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[37] Nonetheless, it has also been stated that the retention of different kinds of data may present different levels of interference with the right to respect private life. Thus, traffic and location data require further safeguards than IP (Internet Protocol) addresses or data relating to the civil identity of users of electronic communications systems.[38]

26. For an EPO to produce transactional and content data, a judge is required, while for subscriber or access data or an EPO-PR, they can be issued also by a prosecutor.[39] An EPO to produce subscriber or access data or an EPO-PR can be issued for any criminal offence, while transactional and content data are subject to stricter requirements to reflect the more sensitive nature of such data and the correspondingly higher degree of invasiveness. EPOs for transactional or content data can only be issued for offences which carry a maximum custodial sentence of at least 3 years or more, exceptions are made for specific harmonised offences for which evidence will typically be available mostly only in electronic form, such as fraud and counterfeiting of non-cash means of payment or attacks against information systems (none goes below a maximum threshold of 1 year).

27. These orders would enable the authorities of member States to seek directly data that is stored by a service provider located in another jurisdiction without going through the authorities of that State. Upon receipt of the EPO, the service provider shall ensure that the requested data is transmitted

transfronteriza: de la orden europea de investigación a las órdenes europeas de entrega y conservación de pruebas electrónicas", *Revista de Estudios Europeos*, vol. 79, 2022, pp. 285-303, p. 299

[36] 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. For a more detailed analysis of this proposal, see A. Gascón Marcén, 'Las órdenes europeas de entrega y conservación de pruebas electrónicas: Evaluación de la propuesta de la Comisión Europea' in Ana Sánchez Rubio (coord.), José Miguel Martín Rodríguez (dir.), Laura García-Álvarez (dir.), *El mercado único en la Unión Europea: balance y perspectivas jurídico-políticas,* Dykinson, 2019 and A. Gascón Marcén, 'Improving access to electronic evidence: the European normative struggle' in *Cybercrime: new threats, new responses,* Huygens, 2020.

[37] Judgment of the CJEU of 8 April 2014, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, and The Attorney General, (C-293/12) and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others (C-594/12)* ECLI:EU:C:2014:238, para. 27.

[38] Judgement of the CJEU of 6 October 2020, *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan and Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v. Conseil des ministres,* C-511/18, C-512/18 and C-520/18.

[39] López Jiménez criticises this distinction because this can give rise to problems since it can happen that a prosecutor issues a EPO-PR, but is not competent to issue the subsequent EPO, if it refers to transaction or content data. And similarly, as the issuance of EPOs relating to these transaction and content data is subject to a series of specific requirements, it may also happen that, once a EPO-PR has been issued by a public prosecutor or even by a judge, however, later it is not possible to request them by means of a EPO, if these requirements are not met. For all these reasons, López Giménez considers that the most logical thing would be to assimilate the issuing authorities and the requirements depending on whether it is a question of obtaining or keeping subscriber and access data, on the one hand; and transaction or content data, on the other. In short, she sees no point in making distinctions between EPOs and EPO-PRs, for these purposes. See R. López Jiménez, "El nuevo marco jurídico transfronterizo de las pruebas electrónicas. Las órdenes de entrega y conservación de las pruebas electrónicas", *Revista General de Derecho Europeo*, Nº. 49, 2019, pp. 307-240, p. 339.

directly to the issuing authority or the law enforcement authorities indicated in the EPO within 10 days. In emergency cases, it must transmit the requested data without undue delay, within 8 hours upon receipt of the EPO.[40] In the Commission's proposal, in most cases, the provider would have been the only one in the position to oppose the execution of an EPO. The direct involvement and responsibilities of service providers in the assessments of law enforcement requests for data is problematic and deserves utmost attention because it cannot pre-empt nor replace the involvement of independent judicial actors, nor substitute for their scrutiny over a cross-border request for access to data.[41] Therefore, a mechanism of notification is very important, as explained *infra*.

28. To cover service providers who are not established in a Member State but offer their services in the EU, the Commission proposed the obligation for them to appoint a legal representative in one Member State.[42] It is feared that this kind of mechanism could be replicated by States who do not respect human rights or the rule of law to get information to prosecute human rights activists or political opposition leaders.

29. Regarding the proposal, Böse recommended: to reconsider whether and to what extent recourse to the European Investigation Order (EIO) could be an alternative option to the creation of the EPO or the EPO-PR, in particular for the disclosure of content and transactional data; that the new cooperation regime should provide for a notification of the Member State in whose territory the service provider is based and, thereby, enable the competent authority of that State to decide on whether or not the order shall be executed; and that the individual to whom the requested data pertains should have a judicial remedy both in the issuing and in the executing States, and he/she shall be informed about the data production and the available remedies in both.[43]

30. Some authors asked for the EU to withdraw the proposal because of the lack of evidence of its added value, necessity and proportionality; its incompatibility with the principles and rules governing criminal justice cooperation; and legal uncertainty.[44] The Meijers Committee also criticized that the proposal lacked binding rules on effective remedies and suggested to consider the possibility of explicitly allowing individuals to bring their complaints before a court in their State of residence.[45]

31. The European Data Protection Board (EDPB) was also very critical. It considered that the necessity of a new instrument compared to the existing EIO or MLA should be better demonstrated, including with a detailed analysis of less intrusive means with regards to fundamental rights such as amendments of these existing instruments or the restriction of the scope of this instrument to preservation orders in combination with other existing procedures to request access to the data. The EDPB also made some suggestions to improve the EPO regarding data protection: the Regulation should provide

---

[40] In the Commission's proposal, it was 6 hours and in the Parliament's negotiating position 16, so 8 hours was a compromise agreed in the trilogue with the Council.

[41] M. Stefan and G. González Fuster, *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 Papers in Liberty and Security in Europe No. 2018-07, CEPS, 2018, p. 50. <www.ceps.eu/system/files/MS%26GGF_JudicialCooperationInCriminalMatters.pdf> accessed 13 November 2022.

[42] 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. This requirement to appoint a representative in one of the Member States of the EU is a common trend in the recent legislation of the EU dealing with digital platforms, see A. Gascón Marcén, "El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea", *Cuadernos de derecho transnacional*, Vol. 13, no. 2, 2021, pp. 209-232.

[43] M. Böse, *An assessment of the Commission's proposals on electronic evidence,* European Parliament 2018, p. 48. <www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf> accessed 13 December 2022.

[44] S. Carrera, M. Stefan and V. Mitsilegas, *Cross-border data access in criminal proceedings and the future of digital justice,* CEPS, 2021.

[45] Meijers Committee, *Comments on the proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters,* CM1809 (2018) <www.commissie-meijers.nl/sites/all/files/cm1809_e-evidence_note.pdf> accessed 13 December 2022.

for a longer deadline to allow the executing service provider to ensure safeguards regarding the protection of fundamental rights; the scope of the Regulation should be restricted to controllers in the sense of the GDPR or it should include a provision that in the event where the service provider addressed is not the controller of the data but the processor, the latter is obliged to inform the controller; the Regulation should include safeguards concerning data transfers in case the service provider would be established in a third country without adequacy decision in this field or refer to the Directive 2016/680 as these safeguards will be applicable; since the mandatory designation of a legal representative differs from the GDPR, the Regulation should precise that the legal representative designated under the e-Evidence Regulation should be distinct from the one designated under the GDPR; and there should be a broader definition of electronic communication data to ensure that the appropriate safeguards and conditions for access to be established cover both non-content and content data.[46]

32. The EDPS supported many of these recommendations and argued that effective protection of fundamental rights in this context requires a degree of involvement of judicial authorities of the enforcing Member State. He therefore recommended involving systematically judicial authorities designated by the enforcing Member State as early as possible in the process of gathering electronic evidence to give these authorities the possibility to effectively and efficiently review compliance of the orders with the Charter of Fundamental Rights of the EU and ensure the obligation for these authorities to raise grounds for refusal on that basis.[47] These are similar ideas than the ones expressed in relation to the EU-US agreement explained *supra*.

33. The Commission proposal had to be adopted through an ordinary legislative procedure. Therefore, it needed the agreement of the Council of the EU and the European Parliament. Within the Council, discussions were centered mainly around the concept proposed by the Commission to serve an EPO directly to the service provider or its legal representative without the involvement of the Member State where the latter is located (i.e., the executing State), the definition of service provider, the immunities and privileges, the review procedure in case of conflicting obligations, and the sanctions for non-compliance with the obligations under the regulation.[48]

34. The problem of the lack of notification to the State was resolved through the incorporation of an article that established that, in cases where the EPO concerns content data, and the issuing authority has reasonable grounds to believe that the person whose data is sought is not residing on its territory, the issuing authority shall submit a copy of the EPO to the competent authority of the executing State at the same time that the EPO is submitted to the service provider.[49] Although the Council reached an agreement on the text to adopt a General approach and negotiate with the European Parliament, this consensus was only superficial because the Member States were divided. In fact, four States fully opposed the transactional text. The most vocal was the Netherlands, which denounced that there was an intense pressure to close the negotiations within the Council quickly and the result opened the way for abuse by EU countries that lack sufficient guarantees over the rule of law and fundamental rights.[50]

---

[46] See EDPB, *Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters*.

[47] EDPS, *Opinion 7/2019 on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters*, 13. <https://edps.europa.eu/sites/default/files/publication/19-11-06_opinion_on_e_evidence_proposals_en.pdf> accessed 13 December 2022.

[48] See *General approach: Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters*, 30 November 2018, Doc. 15020/18.

[49] For a further study on the issue of notification, see T. Christakis, 'E-evidence in the EU Council: the key issue of when one Member State can review the requests from another', *Cross-Border Data Forum*, 1 October 2018 <www.crossborderdataforum.org/e-evidence-in-the-eu-council-the-key-issue-of-when-one-member-state-can-review-the-requests-from-another/> accessed 13 December 2022, and T. Christakis, 'Lost in notification? Protective logic as compared to efficiency in the European Parliament's e-evidence Draft Report', *Cross-Border Data Forum*, 7 January 2020 <www.crossborderdataforum.org/lost-in-notification-protective-logic-as-compared-to-efficiency-in-the-european-parliaments-e-evidence-draft-report/> accessed 13 December 2022,

[50] Financial Times, 'EU Governments approve draft rules on sharing 'e-evidence'', *Financial Times*, 7 December 2018 <www.ft.com/content/63a6105a-fa24-11e8-af46-2022a0b02a6c> accessed 13 December 2022.

35. In a letter signed by several NGOs specialized in the defense of the human rights of Internet users such as Access Now, EDRi or the Electronic Frontier Foundation and addressed to the Member States, they raised several issues regarding the General approach. They considered that: it greatly reduced the possibility for enforcing authorities to refuse recognition and enforcement of an order based on a violation of the Charter of Fundamental Rights of the EU; wrongly assumed non-content data is less sensitive than content data, contrary to case law of the CJEU and the European Court of Human Rights; contemplated the possibility to issue orders without court validation, disregarding what the CJEU had consistently ruled; did not provide legal certainty; and undermined the role of executing States, thereby undermining judicial cooperation.[51]

36. The European Parliament and the Council agreed on a common text through trilogue negotiations, but they were quite difficult. Bertuzzi reported that, while some progress was made on technical details, the provision for notifying the authorities of the executing State remained a blocking issue.[52] He also explained that, since the Council approved its general position in 2018 (it had to be revised), many States had changed their position and opposed the notification system, arguing that it would bring back territoriality and undermine the rationale and effectiveness of the proposal.

37. Twenty-five professional organisations including media and journalists' associations, civil society groups, and Internet companies published an open letter demanding stronger safeguards for fundamental rights for the trilogue negotiations. They asked for a systematic and meaningful involvement of the executing State; protection for lawyers, doctors and journalists; and that all orders were subject to judicial authorization.[53]

38. In its negotiating position, the European Parliament agreed on: adding mandatory notification (only to the executing State); modifying data categories; introducing grounds for non-recognition or non-execution of orders; written consent requirement when the issuing State is subject to Article 7 TFEU procedure on the Rule of law; reinforcing provisions on effective remedies; extending the deadline for emergency cases to 16 hours; and providing for a common EU exchange system with secure channels for the transmission of orders and of requested data.[54]

39. The three last issues to be resolved in the trilogue were: the rules relating to the system for notifying orders, where the Parliament insisted on a mandatory notification system for all orders concerning traffic or content data, irrespective of the basis for the criminal proceedings in the issuing Member State for which those data are required, while the Council was unable to approve such a solution; the rules relating to the data protection regime, for which some technical and substantive issues remained unresolved; and the content of the list of grounds for refusal to enforce an order.[55]

40. The Council managed to impose the 'residence criterion', which means that if the individuals concerned are residents in the Member State issuing the order, there is no need to inform the

[51] See *Joint Civil society letter to Member States about their draft position on "e-evidence",* 5 December 2018). <https://edri.org/files/20181203_e-evidence_civilsocietyletter.pdf> accessed 13 December 2022.

[52] L. Bertuzzi, 'e-Evidence regulation: controversy continues in trilogue discussions', *Euractiv*, 26 May 2021, updated: 2 June 2021 <www.euractiv.com/section/data-protection/news/e-evidence-regulation-controversy-continues-in-trilogue-discussions/> accessed 13 December 2022.

[53] *Joint letter on trilogue negotiations on the e-evidence proposal European media and journalists, civil society groups, professional organisations and technology companies call on decision makers to protect fundamental rights* (18 May 2021). <www.ebu.ch/files/live/sites/ebu/files/News/Position_Papers/open/2021_05_18_EevidenceJointLetter_18May2021.pdf> accessed 13 December 2022.

[54] S. Voronova, "European Production and Preservation Orders for electronic evidence in criminal matters", Legislative Train Schedule, European Parliament, 20 November 2022. <https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-jd-cross-border-access-to-e-evidence-production-and-preservation-orders> accessed 13 December 2022.

[55] Presidency of the Council of the EU, P*rogress report on Regulation on European Production and Preservation Orders for electronic evidence and Directive on legal representatives for gathering evidence,* 23 May 2022, doc.: 8484/22. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9296_2022_INIT&from=EN> accessed 13 December 2022.

authorities of the executing State where their data is stored, and the notification will not be required if the requested information can merely identify a person. In exchange, the European Parliament obtained the suspensive effect of the notification (only for ordinary cases but not emergency ones).

41. EDRi has been very critical of the weakening of the notification system reached by the Council for three reasons. First, no notification is required when the investigative authority seeks subscriber data and traffic data for the sole purpose of identifying the suspect (in most cases, IP addresses). However, identity data can become very sensitive in cases where it discloses the identity of whistleblowers, protesters or investigative journalists and it can put their personal safety at grave risk. Second, the exception to the notification rule when the issuing authority believes that the person whose data is sought is residing on the territory of its Member State leaves the assessment of where the person lives at the sole discretion of the issuing State. This represents a major loophole that can be easily abused to circumvent the notification requirement. Third, the rules to re-use data in other proceedings or to transmit it to another Member State could also be used to circumvent the notification procedure. This undermines the case-by-case review of necessity and proportionality afforded by the notification system.[56]

42. The European Parliament also achieved in the trilogue that the executing Member States might contest the order if it goes against fundamental rights or immunities enshrined in its legal framework, including press freedom. Furthermore, special safeguards from alleged fundamental rights violations have been introduced to refuse orders issued by Member States whose rule of law has been officially called into question in the EU, as is currently the case of Hungary and Poland.[57] Another improvement from the proposal is the creation of a decentralised IT system that will be hosted by the European Commission and will serve to channel the orders to make sure they are authentic and secure.[58]

43. On 28 June 2022, there was an agreement in the trilogue on the core elements of the instruments, including the scope of the notification. Finally, the Council, Parliament and Commission reached a political agreement on 29 November, pending the final vote both in the Council and the Parliament.

III. The Second Protocol to the Budapest Convention

44. As it has been shown in the previous section, States try to improve their access to electronic evidence through different solutions, but this creates conflicts of laws and may position companies in the difficult situation where abiding by one law may result on breaching another. That is why a common solution through international law and particularly a multilateral treaty could be desirable.

45. The Council of Europe seems the perfect framework for this initiative as it is focused on improving the rule of law, democracy and human rights and from this perspective has promoted cooperation in criminal matters.[59] It is important to include human rights expertise in any such endeavor.

---

[56] C. Berthélémy, "e-Evidence" trilogues: what's left of fundamental rights safeguards?", EDRi · 22 November 2022 <https://edri.org/our-work/e-evidence-trilogues-whats-left-of-fundamental-rights-safeguards/> accessed 13 December 2022.

[57] L. Bertuzzi, "EU co-legislators agree on 'key elements' of electronic evidence package", *EURACTIV*, 29 June 2022 <https://www.euractiv.com/section/digital/news/eu-co-legislators-agree-on-key-elements-of-electronic-evidence-package/> accessed 13 December 2022.

[58] L. Bertuzzi, "EU settles rules for accessing electronic evidence across borders", *EURACTIV,* 30 November 2022, <https://www.euractiv.com/section/data-protection/news/eu-settles-rules-for-accessing-electronic-evidence-across-borders/> accessed 13 December 2022.

[59] See the European Convention on Mutual Assistance in Criminal Matters (ETS 30), European Convention on the Transfer of Proceedings in Criminal Matters (ETS 73), European Convention on the Suppression of Terrorism (ETS 90), Criminal Law Convention on Corruption (ETS 173), Council of Europe Convention on the Prevention of Terrorism (CETS 196), Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198), etc.

46. The Council of Europe is quite advanced in looking for solutions to digital problems from a human rights perspective. Currently the work of CAI to create a legal framework for Artificial Intelligence is noteworthy. It also has an important tradition on the matter that started with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), which has been ratified not only by most European States but also non-European States such as Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia or Uruguay.[60]

47. The Convention on Cybercrime (known as the Budapest Convention) is an example of a leader in its field, which is also open to signatories outside of Europe. It has been ratified by 68 States, among them the US, Brazil or Japan.[61] In addition, there are more than 20 States with laws largely in line with the Convention and more than 50 further States drawing on the Convention in their legislation.[62] This means that the Budapest Convention has a global impact.[63]

48. Even if the Cybercrime Convention Committee (T-CY) issued several Guidance Notes aimed at facilitating the effective use and implementation of the Convention in the light of legal, policy and technological developments, it was necessary to update it. The T-CY saw the need to improve access to e-evidence stored in the cloud. The drafting of a Protocol to the Convention was decided in 2017 and finished in 2021, after several rounds of consultations.

49. The Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence provides for: direct cooperation with service providers (Article 6) and domain name registration services in other Parties for the disclosure of information to identify suspects (Article 7); expedited forms of cooperation between Parties for the disclosure of subscriber information and traffic data (Article 8); expedited cooperation and disclosure in emergency situations (Articles 9 and 10); additional tools for mutual assistance such as video conferencing and joint investigation teams and joint investigations (Articles 11 and 12); and data protection and other rule of law safeguards (Articles 13 and 14).[64]

50. The expedited mechanism for cooperation (Article 8) is applied both to traffic data and subscriber information, but not content data. The requested Party, from the date of receipt of the request shall make reasonable efforts to serve the service provider within 45 days, if not sooner, and shall order a return of requested information or data no later than 20 days for subscriber information and 45 days for traffic data. This mechanism does not imply a direct request from the authorities of a State to the intermediary situated in another State, the request passes through the authorities of the second State through a quicker and streamlined MLA process.

51. The Protocol also creates a mechanism for authorities in one Party to directly require data to service providers located in another Party in an analogous way to the EU EPO and the executive agreements under the CLOUD Act already explained. However, this mechanism is limited to subscriber

[60] See O. J. Gstrein, 'The Council of Europe as an Actor in the Digital Age: Past Achievements, Future Perspectives', *Festschrift der Mitarbeiter*Innen und Doktorand*Innen zum*, 2019, pp. 57-90 <www.ejtn.eu/PageFiles/17861/The%20Council%20of%20Europe%20as%20an%20actor%20in%20the%20Digital%20Age.pdf> accessed 13 December 2022.

[61] It has been ratified by all the Member States of the Council of Europe (except for Ireland, which has the intention to do it), but also Argentina, Australia, Brazil, Cabo Verde, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ghana, Israel, Japan, Mauritius, Morocco, Nigeria, Panama, Paraguay, Peru, Philippines, Senegal, Sri Lanka, Tonga and the US.

[62] See Council of Europe, *Cybercrime@COE Update. April - June 2021*. <https://rm.coe.int/cybercrime-coe-update-2021-q2-final/1680a33292> accessed 13 December 2022.

[63] In addition, the Cybercrime Convention Committee (T-CY) has as observers the African Union Commission, the Commonwealth Secretariat, the EU (European Commission, Council of the EU, ENISA, EUROJUST and EUROPOL), INTERPOL, ITU, OAS, OECD, OSCE, UNODC and G7.

[64] *Enhanced cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention* (version 14 April 2021) <https://rm.coe.int/towards-2nd-additional-protocol/1680a22487> accessed 13 December 2022.

information and domain name registration information. Subscriber information[65] is extremely useful for the first steps of police investigations and it is the most often sought out information in criminal investigations. In addition, it is considered less sensitive than content or traffic data, according to the Explanatory Report of the Protocol "it does not allow precise conclusions concerning the private lives and daily habits of individuals concerned, meaning that its disclosure may be of a lower degree of intrusiveness compared to the disclosure of other categories of data."[66]

52. Regarding notification, the Protocol establishes that a Party may require simultaneous notification of any order issued to a service provider in its territory, together with supplemental information and a summary of the facts related to the investigation or proceeding. This issue so controversial in the EU negotiations of the EPO is voluntary in the Protocol and each Party may decide if they require it or not. Nevertheless, it seems highly advisable that the States ask for this notification. The notified authorities can instruct the service provider not to disclose the information given certain conditions. As noted by the European Internet Services Provider Association (EuroISPA) "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."[67]

53. If a service provider informs the requesting authority that it will not disclose the subscriber information sought, or if it does not do it within 30 days of receipt of the order, the competent authorities of the issuing Party may then seek to enforce the order through other MLA mechanisms including the expedited procedure explained *supra*. Parties may request that a service provider give a reason for refusing to disclose the subscriber information sought by the order. As these direct mechanisms are controversial in some cases, the Protocol gives the possibility to the parties to reserve the right not to apply this Article.

54. The drafting process of the Protocol included Parties not subject to Council of Europe instruments on data protection nor to EU data protection rules. According to its Explanatory Report "significant efforts were undertaken to ensure a balanced Protocol reflective of the many legal systems of States likely to be Parties to the Protocol while respecting the importance of ensuring the protection of privacy and personal data as required by the constitutions and international obligations of other Parties to the Convention."

55. Many of the parties to the Budapest Convention are parties to the European Convention on Human Rights and Convention 108, but others do not. The US lacks even a general data protection law.[68] Therefore, an article was included with specific safeguards for the protection of personal data (purpose limitation, quality and integrity of the data, retention periods, automated decisions, sensitive data, data security and security incidents, oversight, judicial and non-judicial remedies, etc.). It is quite a long Article as it tries to distil the essential elements of the EU data protection framework and Convention

[65] Subscriber information is defined as any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: the type of communication service used, the technical provisions taken thereto and the period of service; the subscriber's identity, postal or geographical address, telephone or other access number, billing and payment information, available on the basis of the service agreement or arrangement; any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. Information needed for the purpose of identifying a subscriber of a service may include certain Internet Protocol (IP) address information.

[66] *Explanatory report of the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (28 May 2021), p. 46. <https://rm.coe.int/0900001680a2aa1c> accessed 13 December 2022.

[67] EuroISPA, *EuroISPA's comments on the provisional text of the 2nd Additional Protocol to the Budapest Convention on Cybercrime* (2019) <https://rm.coe.int/euroispa-2929-comments-to-5th-round-draft-provisions-2nd-add-protocol/1680a16180> accessed 13 December 2022.

[68] See M. Barrio Andrés, "La regulación del derecho a la protección de datos en los Estados Unidos: hacia un RGPD norteamericano", *Cuadernos de derecho transnacional*, Vol. 14, Nº. 2, 2022, pp. 186-193. The author gives an overview of the current regime in the United States, that includes sectoral laws and the recent data protections laws approved by some States such as California, and the discussions about the drafting of the American Data Privacy and Protection Act at federal level.

108+.[69] Although Access Now has argued that it may be incompatible with the GDPR for not offering enough safeguards.[70]

56. During the negotiations several rounds of consultations were open to civil society, data protection authorities and industry to comment on the different compromise texts.[71] However, more than 40 NGOs (European Digital Rights, Electronic Frontier Foundation, etc.) urged the Council of Europe's Parliamentary Assembly to give them more time to provide feedback on the Protocol to improve its human rights safeguards as the last round of consultations over the final text only lasted three weeks.[72]

57. Several NGOs have criticized the final version of the Protocol because, in their opinion, it could allow intrusive measures with potential for serious interference with human rights.[73] They are very critical with the direct cooperation mechanism because it encourages the voluntary disclosure of personal data outside of a proper legal framework involving independent judicial authorities in Parties on both sides. In addition, the Council of Bars and Law Societies of Europe (CCBE) stressed that direct private-public cooperation for cross-border data gathering cannot be considered "a satisfactory alternative to judicial cooperation" and these mechanisms undermine the "essential duties of national judicial authorities to ensure that the rights of its citizens are not infringed, compromised or undermined".[74]

58. The NGOs recommended that judicial authorization should be mandatory for all production orders under the Protocol. They also considered that the scope of the definition of subscriber data was overbroad and failed to exclude data categories that would reveal precise conclusions concerning the private lives and daily habits of a subscriber.

59. They also recommended that Parties to the Additional Protocol should be required to accede to Convention 108+. Ideally the parties of the Budapest Convention would ratify Convention 108+ and this would improve data protection in those countries not only because of the obligations that derive from the treaty but also because of the screening process to join it. Most parties to the Budapest Convention are already parties to Convention 108. Nevertheless, it is highly unlikely that all the parties to the Budapest Convention will ratify Convention 108+ in the short term, see, for example, the US. Therefore, it was not a real option that the negotiating States established this as a requirement to ratify the Protocol.

60. Cristina Schulman, Chair of the T-CY, stated that "the process of negotiations was not an easy path", however "it is an outstanding achievement to have reached consensus on an instrument that is breaking new ground and foresees strong data protection standards".[75] The negotiation included experts from the 66 States Parties to the Budapest Convention at the time from Africa, America, Asia-Pacific and Europe. This had as a result a complex text that had to accommodate different perspectives,

---

[69] Convention 108 was modernized by a Protocol amending it in 2018 (CETS No. 223). The modernised version is known as Convention 108+.

[70] Access Now, *Access Now's comments on the draft 2nd Additional Protocol to the Budapest Convention on Cybercrime* (30 April 2021) <https://rm.coe.int/0900001680a25783> accessed 13 December 2022.

[71] Consultations with civil society, data protection authorities and industry on the 2nd Additional Protocol to the Budapest Convention on Cybercrime, <www.coe.int/en/web/cybercrime/protocol-consultations> accessed 13 December 2022.

[72] EDRi, *Civil society warn against rushed global treaty for intrusive cross-border police powers* <https://edri.org/our-work/civil-society-warn-against-rushed-global-treaty-for-intrusive-cross-border-police-powers/> accessed 13 December 2022.

[73] *Joint letter Subject: 6th round of consultation on the Cybercrime Protocol and civil society participation* (2 May 2021) <https://edri.org/wp-content/uploads/2021/05/20210420_LetterCoECyberCrimeProtocol_6thRound.pdf> accessed 13 December 2022.

[74] CCBE, *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) <https://rm.coe.int/ccbe-written-comments-draft-2nd-additional-protocol-to-the-convention-/168098bc6e> accessed 13 December 2022.

[75] *E-evidence Protocol approved by Cybercrime Convention Committee* (31 May 2021) <www.coe.int/en/web/human-rights-rule-of-law/-/e-evidence-protocol-approved-by-cybercrime-convention-committee> accessed 13 December 2022.

legal traditions and constitutional requirements. That is why it has several Articles that include the possibility to reserve its application or ask for additional requirements at the time of signature of the Protocol or when depositing the instrument of ratification, acceptance, or approval.

61. Daskal and Kennedy-Mayo argue that the most dramatic, far-reaching provision of the Protocol is the mechanism for direct cooperation between law enforcement in one country and Internet intermediaries in another, but, in their opinion, even this is a 'modest step' as it applies *only* to subscriber information.[76]

62. Nevertheless, Carrera *et al*. consider that the 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 considering the very broad interpretation that the explanatory report to the draft provision gives to the term 'subscriber information'. They are quite critical with the Protocol and highlight the manifold potential antinomies that it could generate with EU criminal justice and data protection laws, but also with the legal framework established under other CoE instruments, most notably the Convention for the Protection of Human Rights and Fundamental Freedoms and Convention 108+.[77]

63. In the view of Daskal and Kennedy-Mayo, the provisions of the Protocol are a welcome step forward, but need to also come with transparency, oversight, and further protections against abuse. States and many outside observers are worried about a 'law enforcement free-for-all', pursuant to which any government actor anywhere can simply compel production of data anywhere under domestic authority alone. This raises a fear of governments seeking access to data to harass and abuse, rather than investigate legitimate and properly predicated crime. They argue that these are critical considerations to take into account, although the risks can and should be mitigated by the application of and insistence on baseline procedural and substantive rules; careful review, audits and other oversight of the factual predicate for investigations; and refusal by platforms and governments to cooperate with governments that repeatedly violate core rights and freedoms.[78]

64. Spiezia considers that the Protocol will help relaunch the applicative sphere of the Budapest Convention, confirming its centrality in the procedures of international cooperation in the investigation of crimes committed through the Internet and as regards any other form of crime in relation to which the acquisition of digital evidence is necessary. The Protocol reinforces some of the positive aspects that had already emerged in the Convention, such as that of the relationships of suppliers of digital services, whose framework of relations with the requesting authority is definitively clarified. The overall regulatory framework is improved, placing the cooperative dimension at the centre. Spiezia underlines that the tools made available to national judicial authorities have clearly been enriched and applauds that, ultimately, it is the entire new legal framework that moves along the common thread of ensuring greater justice for victims, while ensuring that the risk of accountability for their acts is significantly greater for perpetrators.[79]

65. Alexander Seger, Executive Secretary of the T-CY, stated that "with this Protocol, the Budapest Convention will remain highly relevant and will continue to stand for a free and open Internet,

[76] J. Daskal and D. Kennedy-Mayo, 'Budapest Convention: What is it and how is it Being Updated?', *Cross Border Data Forum*, 2 July 2020 <https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/#_edn21> accessed 13 December 2022.

[77] S. Carrera, M. Stefann and V. Mitsilegas, *op. cit.*, pp. 42-43.

[78] J. Daskal and D. Kennedy-Mayo, op. cit.

[79] F. Spiezia, 'International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime', *ERA Forum,* Vol. 23, 2022, pp. 101-108, p. 104 <https://link.springer.com/content/pdf/10.1007/s12027-022-00707-8.pdf> accessed 13 December 2022.

where restrictions are limited to cases of criminal misuse".[80] This is because the Protocol is considered as the alternative to the Russian sponsored (and China backed) initiative to draft a Convention in the framework of the United Nations to fight cybercrime.[81] This has been criticized by the EU[82] and NGOs because a vague definition of cybercrime could be used to quash political dissent.[83] The EU and the US declared they welcomed the recent approval of the Second Additional Protocol of the Budapest Convention, which remains the "primary instrument for international cooperation on cybercrime".[84]

66. Daskal and Kennedy-Mayo underline that the work on the Protocol to the Budapest Convention happened against the backdrop of this China and Russia-led initiative at the UN to create an alternative cybercrime treaty, framed as an alternative means of asserting sovereignty over the Internet.[85] In their opinion, the data sovereigntist approach was framed as a means of asserting control over the internet and the data needed for basic governmental functions, including law enforcement. The amendments to the Budapest Convention, by contrast, envision a world in which data continues to flow across borders, and seeks to adjust jurisdictional rules to meet these rules, rather than exercise control over the technology to meet pre-established jurisdictional limits.[86]

67. The EU participated in the negotiations of the Protocol trying to ensure compatibility with its own internal initiative to create the EPO. For the EU it has being a difficult process as it had yet to agree on its own internal rules while at the same time was negotiating the executive agreement with the US and the Protocol.[87] The EDPS supported the participation on the negotiations of the Protocol but recommended that the EU opposed any provisions on direct access to data,[88] which obviously did not happen.

68. During the negotiations the EU asked for a disconnection clause to be included that became Article 15. It establishes that the EU Member States may, in their mutual relations, apply EU law governing the matters dealt with in the Protocol. In addition, if the EU and the US reach an executive agreement under the CLOUD Act, as explained in a previous section, this would take precedence over the Protocol to the Budapest Convention in their mutual relations.

---

[80] *E-evidence Protocol approved by Cybercrime Convention Committee* (31 May 2021) <www.coe.int/en/web/human-rights-rule-of-law/-/e-evidence-protocol-approved-by-cybercrime-convention-committee> accessed 23 July 2021.

[81] See Resolution adopted by the General Assembly of the United Nations on 27 December 2019 on Countering the use of information and communications technologies for criminal purposes, A/RES/74/247. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement> accessed 13 December 2022.

[82] *EU Statement in support of the Council of Europe Convention on Cybercrime* (15 January 2020) <https://eeas.europa.eu/delegations/council-europe_en/73052/EU%20Statement%20in%20support%20of%20the%20Council%20of%20Europe%20Convention%20on%20Cybercrime> accessed 13 December 2022.

[83] *Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online* <www.apc.org/sites/default/files/Open_letter_re_UNGA_cybercrime_resolution_0.pdf> accessed 13 December 2022.

[84] *Joint EU-US statement following the EU-US Justice and Home Affairs Ministerial Meeting* (22 June 2021) <www.consilium.europa.eu/en/press/press-releases/2021/06/22/joint-eu-us-statement-following-the-eu-us-justice-and-home-affairs-ministerial-meeting/> accessed 13 December 2022.

[85] Walker and Tennant outline four possible outcomes of the negotiations at the UN. First, a new convention in line with the Russian draft that favours a highly restrictive view on digital sovereignty, data ownership and human rights without the support of the West but with the added legitimacy of being a UN instrument. Second, a compromise convention, leaving political issues such as human rights and sovereignty open to interpretation, that would advance technical capacity programs but will face challenges in monitoring implementation. Third, the alter ego of the Budapest Convention with strong human rights safeguards that would not do much to increase international cooperation across geographies and would not be adopted by some major powers, although it would enhance cooperation between the West and new signatories. Fourth, no result at all, that would represent a failure for multilateralism, but would not significantly change the current order on cybercrime cooperation. S. Walker and I. Tennant, *Control, alt, or delete? The UN cybercrime debate enters a new phase,* Global Initiative Against Transnational Organized Crime, 2021 <https://globalinitiative.net/wp-content/uploads/2021/12/UN-Cybercrime-PB-22Dec-web.pdf> accessed 13 December 2022.

[86] J. Daskal and D. Kennedy-Mayo, op. cit.

[87] C. Brière, 'EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments', *European Papers* Vol. 6, no. 1, 2021, pp. 493-512.

[88] EDPS, *Opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention*.

69. The Protocol was adopted by the Committee of Ministers on 17 November 2021 (CETS No. 224)[89] and opened for signature on 12 May 2022[90]. The EU cannot sign the Protocol, so the Council adopted Decision (EU) 2022/722 of 5 April 2022 authorising Member States to sign the Protocol, in the interest of the EU.[91] Some members of the European Parliament were critical with the Protocol and considered that it lacked some necessary human rights safeguards and wanted the Parliament to ask the Court of Justice of the EU for an opinion to assess the compatibility of the Protocol with the Treaties.[92] Nevertheless, the plenary of the Parliament voted against.[93]

IV. Conclusions

70. The resources dedicated to mutual legal assistance should be improved if they are considered insufficient to fight crime.[94] A study on how the European Investigations Orders have worked in the field of electronic evidence is also necessary. Nevertheless, countries seem to be convinced that the only way to really fulfil their obligation to fight crime and ensure the security of their citizens is to be able to directly gather data from service providers situated abroad. Data localization is dismissed both by the EU and US for its human rights challenges and its problems for electronic commerce and an open Internet.

71. The push for direct mechanisms to gather data is particularly salient currently in Europe with the parallel initiatives of the EU with the EPO and the Council of Europe with the Second Protocol to the Budapest Convention that try to get over the traditional limits of jurisdiction related to the territory of the State. However, human rights should not be sacrificed in the altar of efficiency, so it is necessary to embed the appropriate safeguards in these mechanisms, in particular, in relation to privacy and personal data protection, but also due process, access to remedies, freedom of expression and the confidentiality of communications with a lawyer or journalistic sources. For example, notifying the State affected and giving it the opportunity to reject the order seems a good method to ensure the rule of law and basic standards. We should also be aware of the consequences of this kind of mechanism in the hands of States that do not respect the rule of law.

72. A multilateral solution such as the Protocol to the Budapest Convention seems a superior solution to unilateral ones, *inter alia* because of its scalability. However, it is a pity that, following their desire to reach consensus, the negotiators had to lower some standards and leave some safeguards as a choice for States upon ratification through declarations. This will have as a result fragmenting the regime, as is the case with notifications, for example.

73. We should also be conscious that we are turning Internet intermediaries into human rights adjudicators or defenders[95] when they may be ill-suited for that task. In many cases they would be the

[89] The text is available at: <https://rm.coe.int/1680a49dab> and the Explanatory Report at: <https://rm.coe.int/1680a49c9d> both accessed 13 December 2022.

[90] By 6 December 2022, it has been signed by Andorra, Austria, Belgium, Bulgaria, Croatia, Estonia, Finland, Iceland, Italy, Lithuania, Luxembourg, Moldova, Montenegro, Netherlands, North Macedonia, Portugal, Romania, Serbia, Slovenia, Spain, Sweden, Ukraine, the United Kingdom, Chile, Colombia, Costa Rica, Japan, Morocco, Sri Lanka and the US.

[91] OJEU L 134, 11 May 2022, p. 15–20.

[92] See L. Kabelka, "Controversy surrounds new cybercrime protocol as plenary vote still hangs in the balance", *EURACTIV,* 12 May 2022 < https://www.euractiv.com/section/data-protection/news/controversy-surrounds-new-cybercrime-protocol-as-plenary-vote-still-hangs-in-the-balance/> accessed 13 December 2022.

[93] The results of the votes were: 229 for, 375 against, and 18 abstentions. See European Parliament. Annex. Results of the votes 22/11/2022 <https://www.europarl.europa.eu/doceo/document/PV-9-2022-11-22-VOT_EN.pdf> accessed 13 December 2022.

[94] In this sense, the work of the Council of Europe on the 24/7 Network of Contact Points to fight cybercrime and support MLA is very important, together with the templates for data preservation requests and access to stored data.

[95] See A. Gascón Marcén, "Los intermediarios de Internet y la protección de los derechos humanos" in Jorge Urbaneja Cillán (coord.), Cástor M. Díaz Barrado (dir.), Juan Manuel Rodríguez Barrigón (dir.), Francisco Pereira Coutinho (dir.) *Las empresas transnacionales en el derecho internacional contemporáneo: Derechos humanos y objetivos de desarrollo sostenible,* Tirant lo Blanch, 2019, pp. 399-412.

only ones able to object to the production orders. They need to have enough time to consider requests and we should not create incentives for them to ignore the rights of their users. The trend to make intermediaries the first adjudicator on topics related to human rights does not just affect privacy but also, for example, speech in the content moderation field and its consequences can be far-reaching.