PROTECTING DIGITAL FREEDOM

Recommendations on cross-border access to data

Position paper on the European Commission's proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters

European Digital Rights 20 Rue Belliard, 1040 Brussels www https://edri.org twitter @edri_org tel +32 (0) 2 274 25 70

“The e-evidence proposal must fully comply with the existing EU data protection acquis in particular, as well as EU law and case-law in general.”

- Working Party 29.

contents

EXECUTIVE SUMMARY

EDRi recognises the importance of adequate measures to fight serious crime but is concerned with the direction this file is taking. If adopted, the European Commission's new proposal for a Regulation on European Production and Preservation Orders (the "e-evidence proposal") would have tremendously negative effects on the fundamental rights of affected persons and unsuspected third parties. In an attempt to further speed up cross-border criminal investigations, the Commission overrode the established EU system of judicial cooperation in criminal matters by trying to harmonise criminal law *enforcement* although criminal law *itself* remains one of the least harmonised legal fields in EU.

In this Position Paper, EDRi criticises the new ability of any law enforcement agency in the EU to force service providers in foreign jurisdictions to hand over personal data of individuals without any involvement of the provider's home authorities. According to the Commission proposal, not even the service provider itself—as last resort to protect user rights—would have any meaningful chance to review the legality of any data access request. Instead, EDRi proposes to actively involve national law enforcement authorities in order to protect the right to due process and safeguards such as the restriction of any measures to serious crimes or the principle that any act needs to be considered "criminal" and be similarly punished in both jurisdictions.

We also deplore the confusing definitions of Article 2 which reduce fundamental rights protections for personal data, notably metadata. Instead of inventing new definitions, the EU would do well to follow existing legislation as well as established principles of European case law, according to which metadata can be just as revealing as content data and therefore benefits from the same protections.

Lastly, the e-evidence proposal needs to contain much stronger rules on remedies for affected persons. The right to access effective remedies implies that affected persons first need to know about any data access by (potentially foreign) law enforcement. Therefore we argue that authorities must have a full duty to inform affected persons by default and as soon as possible, except where they provide duly motivated assessments of how that would impede the investigation.

INTRODUCTION

Although the just recently adopted European Investigation Order (EIO), which includes provisions on access to electronic data, has not been implemented yet by Member States[1], the European Commission proposed the new Regulation on European Production and Preservation Orders (respectively EPOC and EPOC-PR) for electronic evidence in criminal matters (e-evidence proposal) on 17 April 2018. The purpose of the proposal is to allow law enforcement authorities in one EU Member State to "seek preservation or production of data that is stored by a service provider located in another jurisdiction"[2]. According to the Commission, the existing EIO is not quick enough for the digital age. At the time of writing, however, there has not been any assessment of the use, efficiency and implementation of the EIO, including its impact on fundamental rights and how the safeguards are being respected (or not) in practice.

The European Parliament's (EP) LIBE committee is expected to put forward amendments and vote on the the e-evidence proposal most likely after the upcoming European elections. European Digital Rights (EDRi) would like to make the following recommendations regarding the provisions falling within our scope of work, i.e. the protection of human rights in the digital environment. EDRi is an association of civil and human rights organisations from across Europe. We defend rights and freedoms in the digital environment.

EDRi supports the aim of achieving a united, coherent and effective response to serious crime and terrorism. However, EDRi is concerned about the worrying provisions it entails and believes this proposal is premature and dangerous. It lowers all the safeguards that were preserved in the EIO but fails to fulfil its own objective of improving "legal certainty for authorities, service providers and persons affected and to maintain a high standard for law enforcement requests, thus ensuring protection of fundamental rights, transparency and accountability"[3]. EDRi therefore encourages MEPs to consider the following recommendations.

---

1 Parliamentary question E-004970/2018 - Answer given by Ms Jourová on behalf of the European Commission, http://www.europarl.europa.eu/doceo/document/E-8-2018-004970-ASW_EN.html.

2 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (p.1), http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2018/0225/COM_COM(2018)0225_EN.pdf.

3 Idem.

1. AN INAPPROPRIATE LEGAL BASIS

The proposal for a Regulation relies on Article 82(1) of the Treaty on the Functioning of the European Union (TFEU)[4] as a legal basis. It provides the framework in which judicial cooperation in criminal matters can be developed in an EU framework, notably by laying down "rules and procedures for ensuring recognition throughout the Union of all forms of judgments and judicial decisions" and by facilitating "cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions." In the impact assessment supporting the proposal[5], the Commission justifies the use of this legal basis by stressing "the principle of mutual recognition" on which European judicial cooperation should be based, thus allowing the authorities of one Member State to directly address an entity that is not an authority in another Member State. This represents a completely new form of mutual recognition among the usual EU's judicial cooperation frameworks, which always imposed two judicial authorities as counterparts in all procedures, one in the issuing State[6] and another in the enforcing State[7]. While the Commission does not provide further assessment of the consequences of the new channel between public authorities and private entities, the chosen legal basis actually proves to be inappropriate to support this "direct cooperation" for two reasons.

4 Treaty on the Functioning of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN.

5 European Commission, April 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A119%3AFIN.

6 The issuing State is the Member State in which the competent authorities issuing the order are located.

7 The enforcing Member State is the Member State in which the legal representative of the service provider executing the order is located.

1.1. Mutual recognition in judicial cooperation cannot exist unless two judicial entities are involved

First, it should be pointed out that "direct cooperation" is a misleading term in the circumstances laid out by the Regulation. The Regulation introduces judicial orders emanating from national judicial authorities in another country that service providers need to execute with very limited grounds for refusal and risk sanctions in the event of non-compliance. Provisions on the execution of these orders only allow for a limited dialogue between the addressee and the judicial authority with an extremely narrow window for service providers to express their concerns. Furthermore, private entities are not judicial authorities. It is therefore inappropriate to talk about judicial cooperation in criminal matters in the sense provided for by Article 82 TFEU as legal basis.

The question is to determine whether the proposed instruments can use Article 82 as a legal basis without the involvement of a second judicial (or equivalent) authority in the first stages of the execution process. In the current version of the text, the enforcing State only has the opportunity to get actual knowledge about the order on two conditions: (1) once the service provider refuses to comply with it and (2) where the issuing authority voluntarily decides to transfer the order and asks the enforcing State to enforce it (Article 14, draft Regulation). Because of the limited refusal grounds as well as the incentives set for service providers to over-comply with the orders, we can expect cases where service providers refuse to comply to be limited to a very small number. In addition, the State which should have knowledge of an order issued by another country will, in the majority of cases, remain unaware of the existence of the order. This procedure does not provide adequate conditions for mutual recognition in the sense of Article 82. Thus, it is doubtful that a Regulation with private entities as addresses of judicial orders without the involvement of a judicial or equivalent authority in the enforcing State will be compatible with current jurisprudence of the Court of Justice of the European Union (CJEU).[8]

RECOMMENDATION

EDRi recommends to review the architecture of the proposed instrument to meet the criteria of Article 82(1) or to review the choice of legal basis of such instrument in case the direct contact regime with a private entity is maintained.

1.2. "Direct cooperation" is incompatible with Article 89 TFEU

It is hard to see how the instruments proposed under the current legal basis comply with Article 89 of the TFEU, according to which extraterritorial jurisdiction such as EPOC or EPOC-PR can only be made "in liaison

8 Opinion 1/15 of the CJEU on appropriate legal basis for the Draft agreement between Canada and the EU regarding the transfer of Passenger Name Record data, http://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&doclang=EN.

and in agreement with the authorities" of the Member State concerned. According to the Commission, its main intention in the draft proposal is to move away from the data storage location in order to establish jurisdiction, "as data storage normally does not result in any control by the state on whose territory data is stored"[9]. Data volatility was prominently put forward to justify the State in which the service provider is offering its services as a better connecting factor to determine the enforcement jurisdiction. However, dismissing the data location criteria and referring to data volatility does not mean we can simply ignore territorial sovereignty.

EDRi argues that data preservation and production are a form of data processing and thus, considered an operation in the framework of judicial and police cooperation. Although this operation is carried out by a private entity, the obligation for service providers to execute an EPOC or EPOC-PR issued by an authority of another Member State constitutes an interference with the territorial sovereignty of the enforcing State, "just as cross-border surveillance and hot-pursuit (Art. 40, 41 Convention implementing the Schengen Agreement) do"[10]. In addition, the proposed model of cooperation foresees neither "liaison" nor "agreement" from the Member State whose territorial sovereignty is violated by an EPOC or EPOC-PR.

By necessity, either the legal basis needs to be changed to allow for the new type of relationship with private entities, or a meaningful notification mechanism needs to be introduced that informs and seeks agreement from the relevant authorities of the enforcing State as well as the affected State. Although the Commission proposal tries to shortcut this, it is crucial to involve the enforcing and the affected States[11] to ensure the respect of fundamental rights and legal principles enshrined in Article 6 of the Treaty of the European Union (TEU), including the rights of defence of persons whose data is being sought. On this basis, Chapter 3 of this Position Paper explains the modalities of introducing such a notification mechanism without overly impairing investigative proceedings.

RECOMMENDATION

EDRi recommends to introduce a notification mechanism addressed to the authorities of the enforcing State and the affected State.

9 Explanatory Memorandum to the e-evidence proposal, p.13.

10 Martin Böse, An assessment of the Commission's proposals on electronic evidence, p. 37 http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf.

11 The affected State is the Member Stat in which the person affected by the order has his or her habitual residence.

2. DEFINITIONS MUST BE ALIGNED WITH EXISTING EU LAW AND INTERNATIONAL HUMAN RIGHTS STANDARDS

In Article 2, the proposed Regulation creates a new categorisation for different types of requested data. In addition to the data types referred to in existing EU and international law[12], namely (1) subscriber data and (2) content data, new categories called (3) "access data" and (4) "transactional data" actually bring some confusion into the Regulation's definitions. The blurred definitions of these two new categories result in differentiated levels of protection and unclear criteria for preservation, production and access. EDRi would like to stress the legal uncertainty this new categorisation of data generates and the gap it creates in relation to established European Court of Human Rights' (ECtHR) and CJEU's case law.

2.1. Definitions need to be more precise and in line with established EU and international law

The definition of what constitutes "electronic evidence" is highly problematic as it assumes that all data requested by an EPOC or EPOC-PR is indeed evidence to be used in criminal proceedings. It tacitly implies that the person whose data is being sought is guilty or will face criminal proceedings. But Production and Preservation Orders under the proposal are not limited to persons suspected in a criminal investigation, and recital 55 suggests that data can be obtained for a fairly large group of persons, except perhaps content data. EDRi therefore recommends to replace the term "electronic evidence" by "electronic data".

12 Such as the Convention on Cybercrime of the Council of Europe and EU Directive 2002/58/EEC.

The four categories (subscriber data, access data, content data and transactional data) of the proposal fail to provide legal certainty and create unjustified overlaps. The Commission defines access data as "data related to the commencement and termination of a user access session to a service" and belonging to metadata in the sense of the Article 4(3) of the ePrivacy proposal[13] currently under negotiation. It claims that "it is appropriate to single out access data as a specific data category". The definitions separate static and dynamic IP addresses, "date and time of use", data related to the "interface used" and the "user ID" from the rest of metadata types. It does so because the former are to be used during investigations "for the sole purpose" of identifying persons, and thus potential suspects. As a result, the Commission is attaching the same lower level of safeguards to access data as to subscriber data in order for law enforcement authorities to determine a person's identity.

However, this distinction (1) between access and subscriber data on one hand, and (2) between access and transactional data on the other remains superficial and non-viable. (1) Subscriber data is not well delineated from access data as they both include IP addresses and data related to the interface used. (2) Access data also significantly overlaps with the definition of transactional data: date, time, duration of use of the service are all covered in both definitions. On top of that, IP addresses could also fall into the transactional data definition ("data on the location of the device") in addition to subscriber and access data. Difficulties to evaluate in which category the requested data belongs prove that this categorisation creates legal uncertainty. What is more, by applying different levels of protection to different types of data, the Commission proposal undermines the appropriate fundamental rights protections for any given set of personal data when it is accessed for law enforcement purposes.

To address this issue, EDRi proposes to keep definitions in line with existing EU legislation[14] and the Cybercrime Convention of the Council of Europe: subscriber data, traffic data and content data. Consequently, static IP addresses permanently assigned to the customer as part of a subscriber agreement should be considered subscriber data and dynamic IP addresses should be considered traffic data.[15]

RECOMMENDATION

EDRi recommends to amend all references of "electronic evidence" into "electronic data" and to align data definitions on the existing international treaty law and EU legislation.

13 European Commission's proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

14 Namely Article 10(2)(e) of Directive 2014/41/EU regarding the European Investigation Order in criminal matters as well as Article 4(3)(c) of the Proposal for a Regulation 2017/0003 concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

15 Douwe Korff, Recommendations for consideration by the Council of Europe Cybercrime Convention Committee, https://edri.org/files/surveillance/korff_note_coereport_leaaccesstocloud%20data_final.pdf.

2.2. Metadata is as sensitive as content data

EDRi is concerned with the introduction of different degrees of safeguards depending on the type of data requested. The Commission proposal is based on the assumption that there is a "different degree of interference with fundamental rights" when law enforcement authorities obtain subscriber data on the one hand, and traffic data and content data on the other hand. In reality, the interference with fundamental rights of a data access does not depend on the data categories but rather on the amount of data and the purpose of access by law enforcement authorities. Worth reminding, the CJEU held that the access of public authorities to personal data retained by internet service providers constitutes an interference with fundamental rights even if such interference cannot be defined as "serious"[16]. In another court case, *Big Brother Watch v. UK*, the ECtHR rejected the British government's argument that communications data (that is to say subscriber and traffic data) was less sensitive than the content of the communications.[17] Indeed, traffic data "could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with"[18]. This statement echoes the CJEU ruling in the *Tele2 Sverige AB and Watson* judgment, in which the Court notes that traffic data and location data "is liable to allow very precise conclusions to be drawn concerning the private lives of the persons, (...) information that is no less sensitive, having regard to the right to privacy, than the actual content of communications".[19] In addition, the CJEU judgment on the Safe Harbour[20] indicates that to determine whether accessing data constitutes "an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences".

By removing most of the legal protections traditionally attached to mutual assistance in criminal matters, the Commission's proposal allows certain categories of personal data to be accessed without any safeguards or limits (see Chapter 4 of this Position Paper), despite interfering with fundamental rights. The only criteria established by the CJEU case law as to when it is justified to have lesser safeguards relates to the access purpose[21]. In this regard, the CJEU emphasised that the objective pursued by the access must be proportionate to the seriousness of the interference with the fundamental rights that the access entails.

16 Ministerio Fiscal case, http://curia.europa.eu/juris/liste.jsf?num=C-207/16, EDRi's analysis of the ruling, https://edri.org/cjeu-introduces-new-criteria-for-law-enforcement-to-access-to-data.

17 Big Brother Watch and Others v. UK, see paragraphs 355 to 357, http://hudoc.echr.coe.int/eng?i=001-186048.

18 Idem, paragraph 356.

19 Tele2/Watson case, paragraph 99, http://curia.europa.eu/juris/liste.jsf?num=C-203/15.

20 Maximillian Schrems v Data Protection Commissioner, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362.

21 Ministerio Fiscal case, http://curia.europa.eu/juris/liste.jsf?num=C-207/16, EDRI's analysis of the ruling, https://edri.org/cjeu-introduces-new-criteria-for-law-enforcement-to-access-to-data.

Consequently, when investigating non-serious crimes, law enforcement authorities should only be allowed to access a limited amount *and* type of personal data – non-serious interference – to solely identify a person. The eligibility of a non-serious offence for which an EPOC can be issued therefore depends on the seriousness of its interference with fundamental rights.

In some cases, a dynamic IP address may not be sufficient to identify who has done what on the internet, notably because a single public IP address is often shared by more than one natural person using the same local network[22]. To identify an actual suspect, competent law enforcement authorities would need much more data from the internet service provider than just an IP address and a specific time period during which it was used. This could be highly revealing about the person's private life and thus, would constitute a serious interference with fundamental rights. The seriousness of this interference should determine whether the access to such data is permitted to fight all offences or serious crimes only.

RECOMMENDATION

EDRi recommends to apply the same level of protection for all categories of data and to respect the principle of proportionality between the seriousness of interference with fundamental rights and the seriousness of the offence to the conditions for issuing an EPOC for subscriber and traffic data.

2.3. Clarifying the scope of service providers

The Commission's proposal defines service providers falling within the scope of the Regulation as "any natural or legal person that provides (...) electronic communications service", "information society services" or "internet domain name and IP numbering services" (Art. 2(3)). Recital 34 also indicates that an order can be addressed to a service provider that provides the infrastructure for data processing and storage to another company or entity if investigative measures addressed to that company would be "not opportune" because it creates "a risk to jeopardise the investigation". In this regard, the wording is vague and unclear. To remain in accordance with the latest EU legislation, EDRi suggests to strictly delineate the type of service providers and the conditions under which they can be covered by the scope of this Regulation. Based on the distinction introduced by the General Data Protection Regulation (GDPR), priority addressees of EPOC and EPOC-PR must be data controllers (Art. 4(7) GDPR). They are bearing the responsibility of data protection obligations and therefore, must ensure the rights of their data subjects are respected. Data processors, on the other hand, only process or store data on behalf of the controller. Considering the interference EPOC and EPOC-PR may have on individuals' fundamental rights, it is important that persons whose data has been preserved and

22 For further details on Network Address Translation, see Douwe Korff, Recommendations for consideration by the Council of Europe Cybercrime Convention Committee, page 7, https://edri.org/files/surveillance/korff_note_coereport_leaaccesstocloud%20data_final.pdf.

accessed are able to exercise their rights. Under the GDPR, this is guaranteed by data controllers and not by data processors.

The exceptional circumstances in which an EPOC should be addressed to a data processor should only be considered given when there are reasonable grounds to suspect that addressing the data controller would impede the investigation. The data processor should inform the data controller once jeopardies of the investigation have been cleared, who in turn should transmit complete information to the persons concerned. Those obligations should be clearly defined in the Regulation and no other exceptions should be provided.

RECOMMENDATION

EDRi recommends to make data controllers the priority addressees for EPOC and EPOC-PR and restrict the conditions for addressing data processors in accordance with the GDPR.

3. A NOTIFICATION MECHANISM TO PRESERVE FUNDAMENTAL RIGHTS, THE INTERESTS OF THIRD COUNTRIES AND LEGAL CERTAINTY

To further elaborate on the necessary involvement of relevant States' authorities, EDRi would like to stress two important added values of a notification mechanism with agreement and for all types of requested data.

3.1 Increasing the protection of fundamental rights

Law enforcement authorities may need efficient and timely access to personal data in order to prosecute persons guilty of serious crimes and support investigations and criminal proceedings. They must ensure, however, that their actions are always within the scope of applicable EU law and in full respect of international human rights standards that protect the persons concerned. This includes the person whose data are being sought as well as the persons whose data are preserved or accessed although they are not the primary target of the investigative measures. The presumption of innocence and the rights of defence in criminal proceedings are a cornerstone of the European Charter of Fundamental Rights within the area of criminal justice. In the current proposal, the responsibility of protecting the individuals' fundamental rights exclusively falls on the issuing authority and, to a limited extend, on the service provider addressed. There is little consideration for the national laws of the enforcing State or the affected State.

3.1.1. The issuing State as sole protector of fundamental rights

The Commission proposal creates three crucial problems that put all power over fundamental rights protections on the authorities of the issuing State alone.

First, according to the proposal, the issuing authority should only issue an order if a similar measure would be available in a comparable domestic situation in their State. Totally excluded from those considerations is the availability of a similar measure in the enforcing or the affected States. In practice, this means the issuing authority could request access to personal data stored in a country where the "crime" under investigation is in fact entirely legal. This leads to an extremely low level of safeguards and a possibility for the issuing authority to bypass protections under the law of the enforcing or the affected States. It also largely undermines the legal predictability for individuals and service providers as both cannot be reasonably expected to know criminal law provisions of all 28 Member States. What is more, in transnational investigations involving law enforcement authorities from several Member States, there is an inherent risk of forum shopping where a particular request for electronic data could always be made from the Member State with the lowest level of safeguards.

Second, an EPOC must not be issued or enforced if the requested data is protected by immunities and privileges under the law of the enforcing State. But again, according to the Commission proposal, the assessment of this is placed solely with the issuing authority which is unlikely to have a sufficiently detailed knowledge of legal immunities and privileges in all EU Member States. Unless the protection by immunities and privileges in the enforcing Member State is apparent, it is reasonable to expect that the law enforcement authorities of the issuing State will bypass this requirement as they are serving their own national interests in a criminal investigation and have little or no incentive to seriously consider the sovereign interests of the other State.

And third, the Commission proposal states that the issuing State shall contact any Member State from which it learns that there may be parallel criminal proceedings ongoing – which corresponds to a vague, non-binding adaptation of the *non bis in idem* principle. This principle usually protects citizens from being investigated (and potentially charged) twice for the same thing – and it should absolutely be binding.

3.1.2 Authorities of the enforcing and the affected State must be involved

What traditionally is considered to be an established ground for refusal of execution in other judicial cooperation instruments is now being watered down to a mere "condition for issuing an EPOC". The problem is that while refusal grounds can be upheld by the enforcing authority, "conditions for issuing an EPOC" entirely depend on the willingness and abilities of the issuing authority to properly verify them. The lack of information that the issuing authority is likely facing is even reflected in the Commission's wording when the proposal says: "If the issuing authority has reasons to believe (...)" (Art. 5(7)). The Commission's objective to bring down obstacles for cross-border access to data cannot undo the factual limits of Member State authorities and therefore comes at a high price: The usual protections granted to citizens by traditional frameworks of cooperation in criminal matters are circumvented or severely weakened.

As a result, the person whose data has been transmitted has no right to challenge the legality, proportionality or necessity of an order before a court of the State of his or her residence. This directly affects the person's right to a fair trial and his or her right of defence, since the person does not benefit from his or her State of residence's role to protect fundamental rights.

In order to ensure that fundamental rights of the person concerned are protected and exercised, including immunities and privileges, and that confidentiality of the information and national security and defence interests are respected, we recommend establishing a notification mechanism seeking the approval of the affected State. This brings the new instruments in line with established principles of judicial cooperation and enables the affected State to fulfil its obligations concerning the protection of fundamental rights recognised in the Charter. Thus, it guarantees that the execution of an EPOC is necessary and proportionate and breaches neither fundamental rights nor the principles of *non bis in idem* and dual criminality.

For the purpose of an efficient, unburdened and timely process, strict deadlines for authorities should frame this mechanism. The decision on the recognition and validation of an EPOC or EPOC-PR should be carried out with the same celerity and priority as for a similar domestic case. We suggest introducing a four-day period to ensure a decision is taken within a reasonable time and to meet procedural constraints in the affected State. In case where the affected authorities do not respond in due time, their liability in relation to the protection of fundamental rights is triggered. Failing to prevent abuses, the affected State can therefore be held responsible by the affected person.

3.1.3 Service providers cannot replace public courts

In the Commission proposal, the only other entity given the opportunity to review and contest an order is the addressee itself. A service provider has ten days to review an EPOC or EPOC-PR and can only refuse to execute it if the order:

- Is incomplete or contains manifest errors;
- Cannot be executed because of force majeure or de facto impossibility (e.g. when the person whose data is sought is not a customer);
- Manifestly violates fundamental rights or is manifestly abusive.

It is legally highly questionable to put the burden of fundamental rights protection into the hands of service providers. Private companies cannot and should not replace the independent judiciary. Neither can we expect service providers to be sufficiently equipped and knowledgable to assess an EPOC's impact on the fundamental rights of an affected person, nor do they have a meaningful incentive to do so.

EDRi believes that this worrying trend of privatised judicial responsibility directly facilitates the circumvention of legal protections. It implies that a corporate lawyer (at best, since many small service providers don't even have that) knows as much human rights law as corporate law and – in less than ten days or even six hours in case of emergency situations – is able to detect potential violations of fundamental rights based on a meagre four-page EPOC certificate. And that certificate would not even include any information regarding the necessity and proportionality of the order nor details about the case.

In addition, the text provides every possible incentive for the service provider to comply and execute an order, without questioning it. While recital 46 creates a safe harbour for service providers who violate the individual right to data protection when executing an order – even under the data protection laws of the enforcing State –, any non-compliance with an order directly implies the risk to face high financial sanctions. Which company (except perhaps the biggest U.S. firms out for a marketing win) would put a user's fundamental rights before their own business interests?

Combined, this legal setup brings the likelihood of any justified non-execution of an order close to zero but it risks making unjustified violations of citizens' fundamental rights common practice.

A notification mechanism including agreement of the authorities in the affected State allows to relieve the service providers' legal representative from the sole responsibility to protect citizens' fundamental rights. It would reallocate the protective function to the authorities best placed to do so.

RECOMMENDATION

EDRi recommends to introduce a notification mechanism including a right to object to the order addressed to the affected State with strict deadlines. Refusal grounds for the affected State should include:

- Conflicts with fundamental rights or inviolable constitutional principles;
- Immunities or privileges;
- The minimum age for criminal acts;
- The non-respect of the dual criminality principle and substantial differences in criminal charges for a same act;
- The non-respect of the definition of serious crime;
- The non-respect of the principle of *non bis in idem*;
- Rules related to freedom of the press and freedom of expression;
- Risks for national security interests.

3.2. A smoother and safer enforcement process

Introducing the notification mechanism with a right to object as explained above solves the problem privatised law enforcement. Nonetheless, the problem of state interests and territorial sovereignty remains. Another notification mechanism should also be simultaneously addressed to the enforcing State to ensure sovereign interests and national data protection regimes are taken in due account. As in the case of the affected State, such notification mechanism should be adjoined by strict deadlines and trigger liability if the competent authorities do not respond within the deadline.

This additional safeguard is crucial to ensure compliance with Article 89 TFEU, which provides that under the legal basis chosen for the Commission's proposal, authorities of one Member State may only operate in the territory of another Member State "in liaison and in agreement with the authorities of that State". What is more, if a service provider fails or refuses to comply with an order, the enforcing State is already aware of the case and already verified it against its own national protection laws. As a result, the enforcement process will be smoother and more efficient while protecting the fundamental rights of the affected person.

RECOMMENDATION

EDRi recommends to involve the enforcing State in the process and to provide a notification mechanism which should include a limited number of refusal grounds to the enforcing State, notably:

- **Conflicts with fundamental rights or inviolable constitutional principles;**
- **The minimum age for criminal acts;**
- **The non-respect of the dual criminality principle and substantial differences in criminal charges for a same act;**
- **The non-respect of the definition of serious crime;**
- **The non-respect of the principle of *non bis in idem*;**
- **Risks for national security interests.**

4. STRONGER SAFEGUARDS FOR THE ISSUANCE AND EXECUTION OF ORDERS

The Commission proposal largely ignores established safeguards attached to traditional international cooperation instruments and thus deprives individuals from the level of protection in the existing international framework of judicial cooperation. The introduction of the recently implemented EIO had initially followed a similar logic: Several traditional obstacles to mutual legal assistance had been first abolished, such as the dual criminality requirement or the *non bis in idem* ('double jeopardy') principle, before being reinstated in the final version of the Directive. The lesson from the adoption of the EIO Directive is that any mutual recognition-based measure that wants to be compliant with EU fundamental rights needs a minimum rights-based and workable list of refusal grounds for non-execution in order to prevent misuse.

4.1. Basic mutual legal assistance principles and thresholds

In any country that upholds the rule of law, and certainly in the EU, any law must be accessible and foreseeable. In the case of enforced measures, a law must provide clear limits regarding the nature, scope and duration of the measure, and define which authority has the power to use and supervise it. EDRi argues that the Commission proposal does not even fulfil these very basic rule of law principles.

Firstly, the draft Regulation requires service providers to review an order, even when that order refer to a foreign legal system, namely the law of the issuing State. Considering how little information such orders are going to contain, especially regarding the type of crime under investigation, it is highly doubtful that the

criminal law provisions on which an order is based are sufficiently accessible to the service provider and the individual concerned.

Secondly, the Commission proposal includes neither a dual criminality requirement nor a clear and fixed catalogue of eligible offences. Any person should be able to know what acts or omissions will make him or her criminally liable and what penalty can be imposed for any given act committed or omitted in his or her country of residence. But it is highly problematic to expect every individual to know all criminal laws of 28 EU Member States when doing something online. When personal data is being accessed through an EPOC and an interference with fundamental rights can be presumed, citizens have a legitimate expectation that the law of the affected State would apply. The contrary would undermine the principle of foreseeability and thus represent a threat to the rule of law. Moreover, national criminal laws evolve and are highly dependent on changing political majorities. For example, as one of very few countries in the EU, Poland presently criminalises abortion by an imprisonment for up to two years[23]. Late political developments in Poland even brought a new abortion law proposal which could have made anyone resorting to abortion punishable by up to five years in prison (the draft bill was eventually rejected in the Polish Parliament)[24].

As a result, accessibility and foreseeability requirements are not sufficiently fulfilled in the Commission proposal. In order to address this issue, EDRi recommends to make dual criminality a requirement for all eligible offences according to which the investigated crime must be punishable in both the issuing State and the affected State.

In addition, the crime should be punished similarly in both States. Because criminal law is one of the least harmonised fields in the EU and remains a domain closely linked to national sovereignty, the principle of mutual recognition can not be fully implemented in judicial cooperation cases. Some national criminal justice systems in Europe even decide whether to prosecute a given crime based on reasons of convenience or opportunity to prosecute. In practice this means that if an offence is classified as less serious or even minor, the State decides not to allocate resources for its investigation if it takes place on its territory. It would be inappropriate to request this State to change its democratic choices in terms of criminal law by allocating resources to support the prosecution of a crime considered as minor, upon the request of a foreign authority.[25] What is more, current examples of rejected European Arrest Warrants show that enforcing States may refuse to execute an order if the accusations by foreign judicial authorities do not match the legal traditions in the enforcing State.[26] EDRi therefore recommends that the refusal grounds available for the

23 The Family Planning, Human Embryo Protection and Conditions of Permissibility of Abortion Act of 7 January 1993, https://www.reproductiverights.org/sites/crr.civicactions.net/files/documents/Polish%20abortion%20act—English%20translation.pdf.

24 Euronews, Abortion laws in Poland (23.09.2016), https://www.euronews.com/2016/09/23/abortion-laws-in-poland.

25 Lorena Bachmaier Winter, European investigation order for obtaining evidence in the criminal proceedings. Study of the proposal for a European directive, 09.2010. http://zis-online.com/dat/artikel/2010_9_490.pdf.

26 See for example the case a Belgian Court refusing to extradite a musician accused in Spain of allegedly insulting the Spanish royal family and "praising terror groups": Bishr El-Touni and Lorne Cook, Belgian

affected State must include the requirement that any offence for which an order is being issued is punishable in a similar way in both the issuing and the enforcing State.

Thirdly, the maximum minimum threshold of three-year imprisonment for an EPOC or EPOC-PR is not a satisfactory safeguard. Unlike the Commission claims in its explanatory memorandum, this definition even covers smaller offences such as simple theft, fraud or assault under the criminal codes of some Member States.[27] It is necessary to include a proper threshold to exclude parts of national criminal codes which do not justify intrusive measures such as EPOC. As argued above, according to the CJEU case law it is crucial to take into account the seriousness of the crime when assessing the seriousness of the interference with the fundamental rights of the individual.[28] The CJEU further explained this requirement in its judgment on the *Ministerio Fiscal* case by providing more details of what constitutes a serious interference in fundamental rights.[29] If the purpose of law enforcement authorities is solely to determine the subscriber's identity, then the interference is considered "non-serious" and therefore, access to personal data can be justified even for pursuing smaller criminal offences (see Chapter 2.2 of this Position Paper). The issuance of EPOC and EPOC-PR should therefore be restricted to serious crimes only, with the exception of cases where the sole purpose of access to subscriber and traffic data is to identify the subscriber's identity. As an alternative, and in order to further harmonise the definition of serious crimes in the EU, the establishment of a list of eligible serious offences could be envisaged.

Fourthly, in case of preservation orders, no limits are provided regarding the duration of the measure. According to Article 10 of the Commission proposal, data can be frozen for an unlimited period of time, waiting for a subsequent judicial cooperation decision (such as an EPOC) to be issued for its production and transfer to the issuing State. Since the proposal does not set any time limit for the issuance of a subsequent EPOC, the service provider could be obliged to keep the personal data indefinitely. The best solution is to set

---

court rules out extradition for Spanish rapper, AP News (17.09.2018), https://apnews.com/6da8638368954bbfaa9c791b994dc4a7.

27 See for instance the maximum punishment for theft, fraud and assault according to §§223, 242, 263 of the German Criminal Code [Strafgesetzbuch] or Art. 222-11. 311-3, 313-1 of the French Criminal Code [Code pénal].

28 See the Tele2/Watson case: "Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 60)." (paragraph 102), http://curia.europa.eu/juris/liste.jsf?num=C-203/15. Digital Rights Ireland case: "Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law. (paragraph 60), http://curia.europa.eu/juris/documents.jsf?num=c-293/12.

29 Ministerio Fiscal case, http://curia.europa.eu/juris/liste.jsf?num=C-207/16 , EDRI's analysis of the ruling, https://edri.org/cjeu-introduces-new-criteria-for-law-enforcement-to-access-to-data.

the maximum time limit for the retention of preserved data to 90 days, which would also harmonise it with Council of Europe's Cybercrime Convention to which all EU Member States are a party.

RECOMMENDATION

EDRi recommends to:

- Introduce the dual criminality requirement for the issuance of an EPOC;
- Add the requirement to have similar prosecution of a crime in both the issuing and the affected States to refusal grounds for execution;
- Add the existence of a reasonable suspicion as a requirement;
- Limit the issuance of an EPOC to strictly defined serious crimes (set out in Annex IV corresponding to Annex D of Directive 2014/41/EU) for any type data requested, except when access to subscriber traffic data is required solely for identification purposes and in accordance with the principle of proportionality;
- Introduce clear and precise provisions on the nature, scope, duration and use of production and preservation orders to limit data preservation and production to what is strictly necessary.

4.2. Prior judicial review by a court or independent administrative authority

The Commission proposal foresees a review by a judicial authority of European Production Orders (EPOC) for transactional and content data, but not for subscriber and access data. As we already ruled out the idea that a degree of sensitivity actually distinguishes metadata from content data, there is no reason to maintain this selective application of a judicial validation criteria. This idea also conflicts with the June 2018 judgement of the ECtHR in the case of Benedik v. Slovenia where the court held that there had been a violation of Article 8 of the Convention related to the failure of the Slovenian police to obtain a court order before accessing subscriber information associated with a dynamic IP address. The blurry definitions for data categories proposed by the Commission further suggest that law enforcement authorities will not be able to determine if a court validation is in fact needed or not for the personal data they wish to request. Judicial review and validation should always be required when it comes to accessing personal data and therefore, when fundamental rights interferences are at stake.

Furthermore, judicial review and validation should only be carried out by a court or an independent administrative authority in accordance with CJEU jurisprudence.[30] The requirement of prior review by a court

30 In the Tele2/Watson case the CJEU ruled that "it is essential that access of the competent national authorities to retained data should, as a general rule, be subject to a prior review carried out by a court or independent administrative body, except in cases of validly established urgency." http://curia.europa.eu/juris/liste.jsf?num=C-203/15.

or an independent administrative body is also emphasised in para. 208 of the Court's opinion on the EU-Canada PNR agreement (case A-1/15). In several EU countries, prosecutors are not independent however but are subordinate to the respective Ministry of Justice. They do not fall within the definition of a court or an independent administrative authority and do not constitute independent judicial oversight for the implementation of the proposed Regulation, as required by the CJEU.

RECOMMENDATION

To set the proposed Regulation in line with CJEU and ECtHR case law, EDRi recommends to require the judicial review and validation by a court or an independent administrative authority for the issuance of an EPOC or EPOC-PR.

4.3. Emergency cases

Time limits for the service provider to execute an order are 10 days in normal circumstances and 6 hours for emergency situations according to the Commission's proposal. However, the definition of emergency is contrary to established case law, according to which an emergency must always be "validly established"[31]. Only in those restricted cases, a prior review carried out either by a court or by an independent administrative body is not mandatory. An ex-post validation should be nonetheless sought by the competent authorities, notably by exposing the reasonable grounds for emergency.

RECOMMENDATION

EDRi recommends to clarify the conditions for issuing orders in emergency cases according to CJEU case law.

4.4. Cost reimbursements

Article 12 of the draft Regulation does not introduce a harmonisation of conditions for reimbursement of the costs induced by the legal review and the identification, collection and production of data carried out by the service providers. In practice, some Member States would propose the reimbursement of these costs according to their national laws while some others would not. We regret that the reimbursement of costs is

31 Tele2/Watson case (para. 120), http://curia.europa.eu/juris/liste.jsf?num=C-203/15.

not streamlined at EU level as we see it as an accountability measure and deterrence against misuse – besides considerations for the capacities of small and medium-sized service providers to cope with the additional administrative burden. If a fee applies to each EPOC and EPOC-PR issued or if the costs induced from the data production were covered by the issuing authority, it would create an incentive for the authority to more clearly define the volume of personal data needed and issue orders with moderation and proportionality.

RECOMMENDATION

EDRi recommends to introduce a minimum costs reimbursement duty for all Member State.

5. CLARIFYING THE RELATIONSHIP BETWEEN SERVICE PROVIDERS AND THE ISSUING STATE

5.1. Dialogue between service providers and issuing authorities

Notwithstanding the notification procedures towards the affected and the enforcing States and following the well-established cooperative relationships among competent authorities, the service provider should be able to enter into a direct dialogue with the issuing authority. Service providers might play an important role in assessing the intrusiveness of law enforcement demands as they are best placed to know about the nature and amount of data requested and the technicalities related to the production and transfer of data. Inappropriate demands or too short time limits should be discussed and reviewed in liaison with the issuing authority. Sanctions should not be placed on service providers who seek clarifications or review of an order in good faith.

RECOMMENDATION

EDRi recommends to allow for a direct dialogue between service providers and issuing authorities.

5.2. Transfer of data between public and private entities

The proposed instrument introduces standardised certificates to ensure the transfer of sensitive information from public authorities to private entities. However, these do not constitute adequate requirements for the authentication of orders and the security of data transfers. Under the proposed rules, service providers will not be able to assess and verify the authenticity of requests from each national competent authority in the EU. Existing practices across the EU regularly show that law enforcement authorities disregard the most elementary security rules. The conditions for the security and integrity of data transfers therefore need to be clarified by this Regulation. For that purpose, orders should contain more information, notably related to the prior review and validation by an independent judicial and administrative authority and belief grounds that the provider is likely in possession of the relevant information.

RECOMMENDATION

EDRi recommends to guarantee security, integrity, authenticity of data transfers between service providers and issuing authorities.

6. EFFECTIVE REMEDIES AND DATA PROTECTION

6.1. Notification to the users and effective remedies

6.1.1. The affected person

Article 11 lays down the modalities for notifying the person whose data is being sought. According to paragraph 2, he or she needs to be informed "without undue delay about the data production". However, this "may be delayed as long as necessary and proportionate to avoid obstruction of the criminal proceeding". This notification requirement to the affected person can very easily be bypassed by authorities since they can pretend it could jeopardise the investigation. No proper justifications needs to be given. In this case, individual rights such as the right to a fair trial are impaired and threatened. Competent authorities need to provide duly motivated and assessed confidentiality restrictions on the disclosure of an EPOC or an EPOC-PR to the individual concerned.

Provisions on judicial remedies are also very limited. As a consequence of the Commission's attempt to leave all fundamental rights protections to the issuing State, the individual whose data has been accessed has no way of challenging the access to personal data before a court of the affected Member State. The proposal provides the individual with the right to defence only once criminal proceedings are launched and only in the issuing Member State (which may well be in a language the affected person does neither speak nor understand). What is more, the proposal does not offer any remedy in cases in which the affected person ceases to be a suspect. This raises some major questions with regard to the accessibility to a fair trial. Legal remedies should also be available to citizens outside of criminal proceedings and in his or her Member State of residence.

6.1.2. Affected persons who are not suspect

Article 3, setting the scope of the Regulation, refers to the broad purpose of supporting criminal proceedings. There is no requirement of a reasonable level of suspicion against the persons whose data is being sought for access or preservation. Article 5 only imposes a general requirement that the order should be necessary and proportionate, and the order should be related to a criminal investigation satisfying the conditions in Article 5(4). Recital 55 indicates that an order will only be manifestly excessive if it concerns an undefined class of people in a geographical area. This broad scope implies that literally anyone's data could be requested. Article 5(5)(c) refers to persons whose data is being requested, not to a suspect and Article 17(1) introduces remedies for persons that are not a suspect or accused person in criminal proceedings.

EDRi is very concerned about the risk of abuse that the possibility for law enforcement authorities to access any person's data even if they are not suspect of a criminal offence entails. Examples of Member States making intrusive or inappropriate requests are numerous, such as requests for information on journalists' phone calls to investigate the source of a leak of confidential information.

Following the CJEU ruling in the *Tele2* judgment (para. 119), access, at least insofar electronic communications data is concerned, can only be granted to "the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime". Exceptions introduced by the Court relate to the protection of vital national security, defence or public security interests from terrorist threats but on condition that "there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities."[32] As a result, the use of the instruments under the Commission proposal should be limited and brought in line with the CJEU's jurisprudence.

Furthermore, when authorities access personal data of a suspected person, they often also access sensitive information about other people with whom he or she was in contact with, revealing i.e. the frequency, time and length or content of a communication. As a result, any such access is likely to be intrusive for unrelated third parties as well. Therefore, EDRi recommends to state clearly the right to effective remedies for affected third parties in the affected State in the operational part of the legislation.

32 Tele2/Watson case (para. 119), http://curia.europa.eu/juris/liste.jsf?num=C-203/15.

RECOMMENDATION

EDRi recommends to:

- Improve the modalities of notification to the affected person;
- Strengthen fundamental rights of the suspect, notably the right to a fair trial and the right to defence: The affected person shall have the right to contest the legality of an order in front of a court of the issuing State and he or she shall have the right to contest the affected State's failure to fulfil its obligations as protective state;
- Limit the access of EPOC and EPOC-PR to data of suspects of criminal offences covered by the Regulation as established in Article 5, excepting when vital national security, defence or public security interests are at stake;
- Provide effective remedies for affected persons who are not suspect.

6.2. Encryption

There is only one reference to encrypted data in the draft Regulation and it is prone to misunderstanding. Recital 19 states that "Data should be provided regardless of whether it is encrypted or not." Service providers are requested to hand over encrypted data to law enforcement authorities, meaning they might transfer more data than necessary and proportionate. As the legislative proposal remains vague and unspecific regarding the use of the data received by law enforcement, it potentially paves the way for national authorities to compel service providers to decrypt information. There are several techniques that law enforcement authorities can use to access encrypted data but there is currently no instance in which encryption workarounds respect fundamental rights[33]. Furthermore, encryption is an essential element of a high level of protection for fundamental rights, especially for the rights to privacy, personal data protection, free expression and due process[34].

RECOMMENDATION

EDRi recommends to delete the last sentence of recital 19.

33 EDRi, EDRi delivers paper on encryption workarounds and human rights (20.09.2017), https://edri.org/edri-paper-encryption-workarounds.

34 Idem.

CONCLUSION

EDRi would like to express its grave concerns with regard to the proposed instruments. The Commission and the Council seem willing to approve this proposal without proper reflections and impact analysis on legal safeguards. The need for timely access to electronic data does not permit bringing down all the fundamental rights protections. Instead, the EU must comply with its own rule of law principles and international human rights standards. The proposal needs meaningful and substantial rephrasing in order to avoid being later annulled by the European courts.

Bearing in mind that the EIO was transposed only one year before the release of this e-evidence proposal, we argue that this proposal is premature. The EU did not take the time to learn from the EIO implementation. Less restrictive alternatives exist and the first step would be to improve the Mutual Legal Assistance treaties to accelerate the procedures and to determine how the EIO can be improved in order to address the problems identified.

Nonetheless and to remain constructive in this discussion, the European Parliament may want to consider the following less restrictive alternatives ranked below according to their intrusiveness in fundamental rights:

GENERAL OPTIONS FOR IMPROVING THE E-EVIDENCE PROPOSAL

Option 1: Narrow the scope of the proposal to subscriber data, in parallel to the discussions taking place at the Council of Europe.
Option 2: Narrow the scope of the proposal to preservation orders only in order to meet the law enforcement authorities' needs and tackle the volatility of electronic data, while introducing clear and precise provisions on the nature, scope, duration and use of these orders to protect fundamental rights.
Option 3: Introduce all the traditional safeguards in judicial cooperation frameworks in accordance to human rights law with clear and precise provisions on the nature, scope, duration and use of these European Preservation and Production orders to protect fundamental rights.