European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

1.4.2019

6th WORKING DOCUMENT (C)

on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Safeguards and remedies

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Birgit Sippel

Co-Author: Romeo Franz

III. Ex-Post Safeguards

1. Effective remedies (Art. 17)

The Working Document has already highlighted that it is very likely that user information only comes at a very late stage of the investigation. Therefore, it is very doubtful whether the data subject, at such a late state of the investigation, can still actually ask for effective remedies. Since this, once again, raises serious doubts as regards the principle of equality of arms and the adversarial principle as parts of the right to a fair trial (Article 6 ECHR), this part of the Working Document will take a closer look at Article 17 of the proposed Regulation, which deals with "Effective remedies".

Article 17(1) of the proposed E-evidence Regulation gives the suspect or accused person the "right to effective remedies against the European Production Order during the criminal proceedings for which the Order was issued".[1] It does not apply to preservation orders (EPOC-PRs). Article 17(2) further stipulates: "Where the person whose data was obtained is not a suspect or accused person in criminal proceedings for which the Order was issued, this person shall have the right to effective remedies against a European Production Order in the issuing State". "Such right to an effective remedy shall be exercised before a court in the issuing State in accordance with its national law and shall include the possibility to challenge the legality of the measure, including its necessity and proportionality." (see Artcle 17 (3).

With this, the proposal does not foresee any rights to an effective remedy in cases of EPOC-PR, neither for the suspect/accused, nor the third parties involved. Thus, as already stated above, in cases where an EPOC-PR is not followed upon by an EPOC, the data subject does not know that its data was preserved and thus does not have any access to remedies at all.

Another issue arises as regards the location where to claim a remedy. Since the proposal stipulates that remedies for suspects and accused can only be claimed "during the criminal proceedings in the issuing state" (Art. 17(1)) and remedies for third persons (Art. 17(2)) only "in the issuing State in accordance with its national law", it is doubtful whether the data subject can actually claim such a remedy. In contrast, as regards the cross-border nature of the proposed e-evidence instrument, it is quite likely that the effective remedy is clearly hampered, due to physical distance to the issuing state, potential language problems, a lack of understanding of the other legal system as well as financial difficulties in claiming remedies in another Member State.[2] The question therefore arises whether the user should not also be able to challenge the legality in the courts of their own Member State (or at least in the Member State of enforcement,

[1] It is stated that this is without prejudice to data protection remedies under without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679.

[2] See also Meijers Committee, CM 1809, 18 July 2018, stating "*Under the proposed mechanism, it is very likely that a situation will arise in which the individual involved - either being a suspect or not - resides in another Member state than both the issuing State and the state on which territory the service provider's legal representative or establishment is placed. Would that not lead to uncertainty under the fundamental rights acquis or otherwise, in which country the individual can lodge a complaint? ... The Meijers Committee therefore suggests to seriously consider the possibility of explicitly allowing individuals to bring their complains before a court in their state of residence."*

as that is where the powers were exercised)?[3]

Furthermore, the proposal does not specify the remedies, leaving it up to Member States to determine as a matter of national law the consequences of a violation of the procedural rules in obtaining electronic data. Looking at previous mutual recognition instruments at EU level, such as the EIO but also the procedural safeguards directives, it has to be admitted that this is a general problem. Until now, those procedural rights directives as well as the EIO miss a clear reference to a harmonised remedy or only use very vague language referring e.g. to the "rights of defence and fairness of the procedure".[4]

2. The question of admissibility of data as evidence

Empirically, seen from the position of the data subject, the only effective remedy seems to be to right to challenge the admissibility of the evidence gathered.[5] This might also help to prevent illegal law enforcement practices, i.e. a misuse of the e-evidence instrument. The mentioned issue relates to the issue of admissibility of evidence in connection with the exclusionary rule.[6] At present, EU Member States vary significantly in their approach to the two mentioned concepts, from a complete absence of admissibility rules to very strict admissibility and exclusionary rules.[7] According to practitioners, as regards their application, they even heavily vary from court to court and judge to judge. And also at EU level, there is no clear legal framework as regards the admissibility of evidence, which makes the principle of mutual recognition difficult to operate. Currently, the only common basis stems from ECHR case-law whereby clear rules were established on violations of Article 3 ECHR (prohibition of torture, inhuman and degrading treatment).[8] However, as regards the right to a fair trial (see Article 6 ECHR, including, among others, the right to remain silent, right to a lawyer, right to defence,

[3] Compare to Articles 50 and 52 of Directive 2016/680 ("Data Protection Police Directive" - right to lodge a complaint with a single supervisory authority that the data subject chooses, and transmission by it to the competent supervisory authority).

[4] The e-evidence Regulation goes a step further in Article 18 as regards ensuring privileges and immunities, as well as fundamental interests of the enforcing state, but only for transactional or content data. However, it is only the court in the issuing State that shall ensure during the criminal proceedings for which the Order was issued that these grounds are taken into account in the same way as if they were provided for under their national law when assessing the relevance and admissibility of the evidence concerned. In view of the different systems the consequences might be substantially different and not the same as they would be in the state of enforcement. The Council general approach deleted Article 18.

[5] See, for example, comparatively judgments of the US Supreme Court in *Wolf v. Colorado*, 338 U.S. 25 (1949), opting for a divergent system of sanctions in the federal states, and overruled in *Mapp v. Ohio*, 367 U.S. 643 (1961) introducing the exclusionary rule as a common effective remedy in all federal states to prevent violations of the 4th Amendment prohibiting illegal searches and seizures. See also Fair Trials International, Consultation paper on e-evidence, February 2019 stating (p.1): *"A key check on the legality of evidence-gathering by law enforcement authorities occurs at trial (or shortly before, after the evidence has been gathered). This is the power for the accused to challenge the admissibility of evidence on which the state is seeking to rely to secure a conviction. The accused person must have the right to challenge the request and use of data at trial, and seek specified appropriate legal remedies where electronic evidence has been obtained illegally. And in order to be in a position to exercise the right to challenge, accused persons must be able to obtain disclosure of the sources of the electronic evidence."*

[6] The two concepts are connected but not identical. Admissibility refers to the issue of the possibility to base the judgment on certain evidence or not. The exclusionary rule, in addition, demands that in principle the judge that adjudicates the matter at the trial stage should not be in contact with inadmissible evidence as this could trigger his/her psychological contamination.

[7] See, for example, S. C. Thaman, Exclusionary Rules in Comparative Law, 2012.

[8] See, for example, ECtHR, *Gäfgen v. Germany*, a. no. 22978/05, judgment of 1 June 2010, and *El Haski v. Belgium*, a. no. 649/08, judgment of 25 September 2012.

etc.[9]) or the right to privacy (see Article 8 ECHR), the rules are much less clear and only refer to a weighting principle on "fairness of the procedure as a whole" on violations of the mentioned rights. Even relevant case-law on Article 8 ECHR (in connection with admissibility and fair trial in Article 6 ECHR), as developed by the ECtHR, is based on vague criteria that are much below the current standards in several Member States.[10]

Consequently, the new mechanism must specify which remedy applies where electronic evidence has been obtained illegally. Further, in order to prevent law enforcement authorities from benefitting from illegally obtained evidence (e.g. if only the illegally obtained evidence secures a conviction), the proposed new tools need to enable a review of the way in which evidence was gathered. To this end, the underlying source of the electronic data must be disclosed to the reviewing court and to the defence to enable an assessment as to whether electronic data was gathered lawfully and how exculpatory evidence can be obtained. If it has been proven that evidence has been obtained illegally, new rules as regards the inadmissibility of such evidence have to be introduced or, at least, certain harmonisation of national admissibility/exclusionary rules.[11]

3. Prohibition to further processing and onward transfer of evidence

A prohibition of use of the evidence outside the investigation procedure and in particular a prohibition on disclosure of data to investigating authorities which are not associated with the case, should be introduced. The transfer of data for public security purposes should be clearly regulated. The proposed system is a criminal law system and should not be used for intelligence purposes due to the trend in some Member States to blur the line between law enforcement and intelligence. This is necessary in cases where a person concerned has been able to obtain a decision that an EPOC had been issued improperly (Art. 17). If the data, which were later found as illegally obtained, had already been passed on, their deletion can hardly be carried out and controlled.

Separate procedures would have to be created for recovery and transfer in cases where the investigation is still on-going and the measure is still concealed. Here, the courts of the enforcing Member State should take such decisions on onward transfers and disclosures. In particular, before passing on the data to authorities of third countries, a judicial decision by courts of the enforcing state is indispensable.[12]

[9] In addition, the mentioned ECHR standards are much lower than most Member States' constitutional and EU standards. For example, the right to remain silent is only a relative right according to ECHR case-law (see, for example *John Murray v. UK*, a. no. 18731/91, judgment of 8 February 1996) but an absolute right in the EU (see Directive 343/2016 and some national constitutions). See, for example, *Bykov v. Russia*, a. no. 4378/02, judgment of 10 march 2009, as regards criteria for assessing fairness of the procedure for a potential violation of the right to remain silent.

[10] See, for example, ECtHR, *Malone v. UK*, a. no. 8691/79, judgment of 2 August 1984, *Schenk v. Switzerland*, a. no. 10862/84, judgment of 12 July 1988, *Kopp v. Switzerland*, a. no. 23224/94, judgment of 25 March1998, *Khan v. UK*, a. no. 35394/97, judgment of 12 May 2000, etc.

[11] The European Parliament already took this approach in its internal position for negotiations as regards certain aspects on presumption of innocence proposing a strict non-admissibility in cases of violation of the right to remain silent (legislative procedure on Directive 2016/343).

[12] Deutscher Richterbund, ibid.

4. Financial compensation and penalties

Furthermore, it should be assessed whether effective remedies could also actually include financial compensation for the data subject, if covered by the legal basis. With such a compensation regime, also third persons who are not a subject/accused and, thus, where the question of admissibility of evidence does not play a role, could thereby actually profit from an effective remedy. Apart from the question of admissibility, in order to prevent law enforcement authorities to unlawfully obtain evidence, it might be worth wise to examine the possibility to also foresee penalties for issuing authorities which unlawfully requested data (compare, for example, Art. 57 Police Directive), if covered by the legal basis.

5. Remedy for Service Providers

As private entities, service providers are rather ill-equipped and have no intrinsic incentive to protect the fundamental rights of their users. Service providers thus cannot and should not be brought in the position of having to replace public authorities as regards fundamental rights protection.

Stakeholders have nevertheless pointed at the importance of giving service providers the realistic opportunity to refuse the execution of an EPOC or EPOC-PR if they have reasonable grounds to believe that such order may be illegal.[13] It has been questioned why only a "manifest" violation should be one of those refusal grounds, and not simply "a violation". Also, for this to work, service providers would need enough time to assess a request and should not be one-sidedly threatened with extremely short time limits and financial sanctions for it.

IV. Effective Oversight and Public Accountability

1. Effective and systemic oversight on the use of the measures

If the new tools are used fairly and proportionately, they are more likely to maintain public trust in criminal justice systems and law enforcement authorities. Effective oversight mechanisms will have to ensure that they insulate against the risk of improper use, and, thereby, help protect both the reputation of legitimate law enforcement activity and those who could become victims of abuse of the tools. To this end, oversight bodies for cross-border production of evidence, should be involved as part of an adequate institutional set-up (EIO model, EDPB model, JPSG model, or perhaps national models), including real powers of oversight.

2. Transparency and Accountability

Article 19 of the proposed Regulation refers to the issue of "Monitoring and reporting" laying out concrete obligations on the Commission and the Member States in order to monitor the outputs, results and impacts of the proposed Regulation and to collect a wide variety of data. Such a provision presents an added value.

[13] EDRi position paper.

Statistics are a re-occurring problem in the field of EU criminal law, as Member States in legislative negotiations often want a more limited set of statistical data in comparison with the European Parliament and the Commission.[14] However, such data is essential in order to address, *inter alia*, potential problems with excessive and unfounded orders, and to be able to assess the functioning of existing instruments. Consequently, Member States should not only collect and report statistics to the Commission (as foreseen in Art. 19(2)), but such statistical data needs also to be publicly published. Furthermore, there seems a need to expand Article 19(2) to also cover more detailed information:

- number of EPOC(-PR)s issued and indication to which other Member States,

- indication of type of criminal offences for which EPOC(-PR)s were issued,

- and number of convictions in cases where EPOC(-PR))s were used.

V. Limitations of safeguards and the so-called "right to security"

In its impact assessment for the e-evidence proposal, but also in other proposals since the entry into force of the EU Charter of Fundamental Rights, the Commission states that, based on Article 6 of the Charter, a "right to security" exists and that such a right, as it seems, would have to be balanced out against other individual rights and safeguards.[15]

This argumentation, however, has to be vehemently rejected, because any reference to Article 6 of the Charter is misleading and wrong. Neither under ECHR, nor under the Charter does any legally recognised "right to security" exist. The mentioned Article does not introduce two separate rights, as stated by the Commission, namely right to liberty and right to security, that have to be balanced. By contrast, Article 6 of the Charter is a mere reflection of Article 5 ECHR (with exactly the same title) which clearly refers the right to be secure from State's unlawful detentions. Thus, there is no separate legally recognised right to security.[16] There is security as a basic human need[17] but it is not a legally recognised fundamental right neither under the ECHR nor under the Charter.

Under the ECHR, in certain articles, only the concept of positive obligations of the Contracting Parties exists, for example in Article 2 (right to life)[18] or Article 3 (prohibition of torture, inhuman and degrading)[19], whereby, in some particular cases, Parties to the Convention can be responsible for violating such positive obligations. However, such obligations do not form a kind of penumbra (shadow) "right to security". In addition, Article 52(3) of the Charter

[14] Compare, for example, the initial Commission proposals and the final legislative texts of Article 11 of Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union and Article 35 of Regulation 2018/1805 on the mutual recognition of freezing and confiscation orders.

[15] In e-evidence it is connected with the issue of victims. However, in other Commission's documents it seems as a free standing right. See, for example, Commission Staff Working Document on Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and the Council on combating fraud and counterfeiting of noncash means of payment and replacing Council Framework Decision 2001/413/JHA.

[16] This was clearly pointed out by FRA as well as by the EU Network of Independent Experts on fundamental rights *("During the drafting of Article 6 of the Charter in the Convention, the term 'security' has repeatedly led to controversial discussions, and some members proposed to simply delete it, as it might give rise to different interpretations in some EU member States, such as France, Italy and Germany. The Convention, however, decided to maintain the term in the restrictive understanding of the Strasbourg case-law under Article 5 ECHR."*)

[17] See A. Maslow, Motivation and Personality, 1954.

[18] See, for example, ECtHR, *Osman v. UK*, a. no 23452/94, judgement of 28 October 1998.

[19] See, for example, ECHR, *Z. and Others v. UK*, a. no. 29292/95, judgment of 10 May 2001.

stipulates that "in so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection". Consequently, rights and safeguards cannot fall below the level of the Charter. However, the Commission's reference to their artificial, non-existing "right to security" is used in the proposal in order to balance those right and safeguards at a different and possibly lower level than ECHR.

Clarification on this issue is important, as it seems that due to the use of this legally non-existing term, inter alia, by the Commission, the balancing of rights and safeguards (as a derivate of individual rights, like the right to an effective remedy, access to a court, fair procedure, limitations of privacy, right to be informed about charges, equality or parties principle, etc.) started to be affected in comparison with ECHR standards.[20]

Conclusion

- Ex ante remedies have to encompass strict conditions for issuing EPOC(-PR)s, such as a certain evidence standard reached and a certain duly assessed level of proportionality, whereby also the provider should be able to provide a certain test.

- In order to allow the affected person to make use of any available remedies, he or she has to be aware about the measure and the fact that his/her data was produced/preserved, in order to guarantee the right to defence and to a fair trial. Therefore, a much more meaningful notification has to take place, at least at the state of enforcement, including a fundamental rights clause based on the EIO example. Confidentiality has to be the exemption, not the rule, and has to be governed by strict conditions.

- As regards potential violations of the rules laid out in this Regulation, the text also has to foresee access to effective legal remedies. Consequently, more harmonised rules on the remedies available in the issuing state as well as on the admissibility of unlawfully collected evidence and the exclusionary rule, as flanking measures. Additionally, access to remedies in the country where the data was produced/preserved or in the Member State where the suspect or the third person resides as well penalties for authorities unlawfully issuing EPOC(-PR)s might be necessary to actually allow for effective legal remedies.

[20] See also CJEU, Case C-601/15 *J.N* . v. *Staatssecretaris van Veiligheid en Justitie,* judgment of 15 February 2016, para. 45 ("the explanations relating to Article 6 of the Charter […] make clear that the rights laid down in Article 6 of the Charter correspond to those guaranteed by Article 5 of the ECHR"). Unfortunatelly, the CJEU itself created some confusion by unclear references in opinion 1/2015 and Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others.* In the future the CJEU shall be more careful in that regard not to trigger misunderstandings with negative consequences for the compliance of the Charter with ECHR minimum. See also X. Tracol, Opinion 1/15 of the Grand Chamber, Computer law & security review 34 (2018) ("*The reliance by the Grand Chamber on Article 6 of the Charter in this specific context is unpersuasive and its implications are unclear"*).

- The issue that the legal representative might be decoupled from the place of establishment of the service prover has to be further analysed, as it has significant impact on the other Member State that has to be notified. It also has to be clarified if such a system is indeed also necessary for EU-based service providers (or if it would not only be necessary for third-country based service providers), in particular regarding existing cooperation instruments as well as the ECHR and EU fundamental rights and data protection framework.

- Transparent and public monitoring and collecting of statistics has to be part of the system.

- There is no legally recognised "right to security" under Articles 5 ECHR and 6 of the Charter and any balancing test as regards fundamental rights shall not adhere to such a non-existent right.