European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

1.4.2019

6th WORKING DOCUMENT (B)

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

II. Ex-Ante Safeguards

After having analysed the proposal as regards the notification of the data subject, this Working Document will now examine those safeguards which have to be guaranteed before data is gathered and transferred to the requesting state (so-called ex-ante safeguards).

Since the question of prior authentication of EPOC(-PR) by the service provider (guaranteeing that an EPOC(-PR) was actually issued from an competent judicial authority) has already been thoroughly been discussed in the 3rd Working Document[1], this paper will only focus on ex-ante safeguards with regards to third parties as well as those related to the enforcement procedure.

1. Third parties affected[2]

It is almost inevitable that even the use of targeted EPOCs will result in an incidental collection of data of persons with whom the originally intended data subject, i.e. the suspect/accused, has communicated. Some of this information may be relevant to the investigation, some not. Consequently, not only the preservation, production and dissemination of data targets but also of third-party data (including the security of the data) have to be governed by strict rules, which ensure the full guarantee of fundamental rights and data protection principles. However, such issues regarding the retention, dissemination, and security of collected data have not been adequately considered or addressed to date. Apart from a very basic common understanding that data has to be adequately protected against hackers and other nefarious actors, there is a need for a clear set of rules and procedures regarding how long collected data can be retained, with whom it can be shared, and for what purposes, before the data is gathered and transferred to the requesting state.

2. Notification and possible reaction for authorities in the state of enforcement

Another important element as regards ex-ante safeguards refers to the question of a stronger involvement of the authorities of the state of enforcement, including a comprehensive notification about an EPOC(-PR) and possibility of a meaningful reaction or even a prior authorisation. This issue has already been highlighted in several of the previous Working Documents. Such an automatic right of the enforcing authority to react is currently not foreseen in the Regulation proposal. Even though Article 14(4)(f) and (5)(f) include a provision stating that a service provider might not comply with an EPOC(-PR) where "it is apparent that it manifestly violates the Charter or that it is manifestly abusive", it presupposes that the service provider has not complied with an EPOC(-PR). Only then, the authorities of the executing state would be getting an active role.

Yet, in order to guarantee the current ECHR jurisprudence and obligations for Member States, a stronger involvement of the executing state seems to be the only rational solution.[3] Such a

[1] See also BRAK (Bundesrechtsanwaltskammer), Nr. 28/2018 referring also to the necessity of a broader set of data to be sent to the providers mirrored on Article 5 EIO.

[2] Any access to third parties data that are not suspects shall be even under more strict conditions, such as limited to exceptional access only, for example, for the protection of vital national security, defence or public security interests.

[3] See WD 3.

possibility of notification and reaction could be modelled on Article 31 EIO and the non-recognition grounds listed in Article 11 EIO and could be adapted to the different categories of data.

As regards subscriber and access data, such a stronger involvement could stipulate that an EPOC(-PR) is sent automatically and at the same time to the service provider and the authority of the enforcing state, the authority of such state would have a certain time limit to object to the EPOC(-PR) based on Article 11 EIO non-recognition grounds.[4] As such, instead of requesting the confirmation of an EPOC(-PR) by the authorities of the enforcing state, EPOC(-PR) on subscriber and access data would give the right for negative reaction to the enforcing state.

As regards more sensitive categories of data, i.e. transactional and content data, a stronger involvement regime may require stricter obligations, for example a positive decision and, thus, a confirmation, of the enforcing state of an EPOC(-PR) before the data is being produced/preserved.[5]

Furthermore, as regards the wording of the fundamental rights clause, instead of applying the very vague wording used in the Commission proposal, namely "manifestly violates the Charter of Fundamental Rights of the European Union", the definition from the Article 11(1)(f) EIO shall be used ("there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter").

Taking over the same wording as in the EIO seems to be even more important in order to overcome the current patchwork of clauses from different EU mutual recognition legal instruments and CJEU case-law.[6] Even though it has become clear over time that a clear fundamental right clause is essential for guaranteeing fundamental rights obligations, the practice has rather been to introduce different clauses for each mutual recognition instrument, with a clear intention by some to limit it or render it inapplicable.[7] Therefore, a fundamental rights clause has to be sufficient broad to be able for a judge to use it if necessary (he or she has a duty to protect fundamental rights), referring to all rights (not only a catalogue of rights)[8] and shall refer to Article 6 TEU.[9] Only with this future court referrals and

---

[4] As regards the use of Article 11 EIO see also CCBE position on the Commission proposal, 19 October 2010.

[5] The Council general approach does not solve the issue with the introduction of a new Article 7a with a notification as regards content data and where a person is from the state of enforcement, There is no clear cut prerogative of the enforcing state to intervene, either in a negative way (a certain deadline to react) or in a positive way (an authorising decision). The issuing state will any possible concerns (in a very limited number of cases) only possible take into account. See also CCBE recommendations on e-evidence, 28 February 2019.

[6] See, for example only a general reference in Article 1(3) of EAW Framework Decision 2002/584/JHA and explicit clauses in several Member States when transposing it; Article 20(3) of Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties; Article 11(1)(f) of the EIO Directive; Articles 8(1)(f) and 19(1)(h) of Regulation 2018/1805 on mutual recognition of freezing and confiscation orders as well as *Aranyosi and Căldăraru*, joined Cases C-404/15 and C-659/15 PPU, and *Minister for Justice and Equality v LM*, case C-216/18 PPU.

[7] For example, by using the term "flagrant denial of justice" (an ECHR concept mainly used as regards extradition to third states) that was explicitly refused by the EP in the EIO negotiations due to its extreme limitations.

[8] Some Member States wanted to limit categories of rights covered by such ground as regards the mutual recognition of freezing and confiscation orders. However, the EP strongly objected to a limitation to certain rights only. See also EDPB, ibid, stating (p. 17): *"Even the ground to refuse to enforce an order on the ground that it would violate the Charter appears higher than the classic threshold relating to a breach of the fundamental rights of the person concerned. Consequently, ... the draft Regulation should at least foresee the minimum classic derogation that if there are substantial grounds for believing that the enforcement of an order*

fundamental rights tensions can be avoided.[10]

3. Notification of the *affected* State

The approach of the Commission Proposal to provide the authorities of the issuing State with direct legal power over service providers (and thus citizens' data) with only limited or late notification of the affected person, leads to a situation in which the affected person has no effective possibility to challenge the legality, proportionality or necessity of an order before a court accessible to him or her in the State of his or her residence. This directly affects the right to a fair trial and the right of defence. Thus, the so-called "localisation of target" parameter, whereas the location of the data subject (in addition to the place of prosecution) should be taken into consideration, would not be followed by the Commission proposal.[11]

One way to ensure that the fundamental rights of the person concerned can be effectively exercised, including immunities and privileges (i.e. for journalists, doctors or lawyers), would be to establish a notification mechanism through which the issuing State informs or seeks the approval of the affected State before issuing an order to the executing State and the service provider. This would bring fundamental rights protections up to the established standards of judicial cooperation and enables the affected State to fulfil its obligations with regard to the protection of fundamental rights.

However, the main question arises which State shall be notified, namely the State where the data is stored, the State where the legal representative of the service provider has been appointed, the State of residence[12] of the affected person or/and the State of its nationality?[13] The issue becomes even more complicated with the notion of a representative introduced with the parallel Directive, whereby such a representative might differ from the seat of the provider in the EU and the place where the data is stored in the EU.[14] In theory, it seems that, in order to be in line with EU/ECHR fundamental rights/data protection obligations, all of those would have to be informed. To keep the necessary efforts as low as possible, an option could be to stipulate the appointment of a legal representative only for third states providers; for EU providers, the current system, whereby in principle, the seat of the provider/the data location

---

would result in a breach of a fundamental right of the person concerned and that the executing State would disregard its obligations concerning the protection of fundamental rights..."

[9] A reference to Article 6 TEU is important as it refers to three layers of fundamental rights protection, namely ECHR, Charter and common constitutional traditions. By such a reference also a potential "Solange" clash between national constitutions and EU law as regards fundamental rights protection can be avoided.

[10] In Member States mutual recognition instruments are often transposed with a special law. It does not make sense and it is non-workable for a judge that for each different mutual recognition procedure a different fundamental rights clause (either broader or limited would be used), for example one for the European Arrest Warrant, one for confiscations, and one for evidence. A judge does not work and assess cases like this - either he or she sees a risk or he or she does not see a risk for fundamental rights.

[11] See, for example, Council WK 3901/2017, Belgian proposal for a working methodology stating "In our view, it represents the most relevant 'connecting factor' apart from the ground for prosecution", whereby the notion of "location of the habitual use of the service by the target" has been proposed.

[12] For this option see T. Christakis, CBDF, "Big divergence of opinions" on e-evidence in the EU Council: A proposal in order to disentangle the notification knot.

[13] Ibid.

[14] See Article 3 of the proposed e-Directive ("The legal representative shall reside or be established in one of the Member States where the service provider is established or offers the services."). The system would be logical for providers not established in the EU but offering services in the EU. However, as regards providers established in the EU it creates a change to the current practice and to a functioning system of cooperation. This was raised by the German judges association - see Deutscher Richterbund, Stellungnahme Nr. 6/18.

serve as point of contact, might be more suitable. In this regard, it seems questionable that the Council general approach on the e-evidence Directive of 8 March 2019[15] tries to extend, as it seems, the notion of legal representative (and all questions connected with this as regards notification) to other existing instruments, like the EIO. With such a potential extension a current working and established system as regards EU providers would be put into question.[16]

In addition to the question of the necessary addressees of a comprehensive notification, another important aspect concerning the potential consequences of such a notification. At least for some categories of data, such a notification must include the possibility to react, at least in a negative way (i.e. to block the measure in a certain time based on the model of Article 31 EIO) in order to allow for the enforcing state's responsibilities under the ECHR system as well as in view of the sensitive nature of some data in line with CJEU case-law (especially, as regards the very low threshold used by the Commission, for example, on trafficking data).[17]

4. Different safeguards for different categories of data (Art. 2)

The Commission introduced four categories of data in its proposal: (a) subscriber data, (b) access data, (c) transactional data and (d) content data. The proposal attaches various requirements depending on the categories in which the data sought by the competent authorities falls. While subscriber and access data only require the validation by a prosecutor and can be accessed for all criminal offences, transactional and content data can be accessed only with prior validation by a judge and for criminal offences punishable by a maximum of at least three years of imprisonment, for offences harmonised in Council Framework Decision 2001/413/JHA, Directive 2011/93/EU and Directive 2013/40/EU as well as terrorist offences listed in Directive 2017/541/EU.

Two issues arise in relation to the new data categorisation: (1) the definitions partly overlap (see definitions for access and transactional data) and risk impeding the rightful use of the instruments by law enforcement authorities; (2) the categorisation departs from definitions of

[15] Council, doc. 6946/19.

[16] See Recital 8 of the mentioned general approach stating: *"The legal representative at issue should serve as an addressee for domestic orders and decisions and for orders and decisions pursuant to Union legal instruments adopted falling within the scope of Title V, Chapter 4, of the Treaty on the Functioning of the European Union for gathering evidence in criminal matters, including where those orders and decisions are transmitted in form of a certificate. This includes both instruments that permit the direct serving of orders in cross-border situations on the service provider or its legal representative, such as the [Regulation on European Production and Preservation Orders for electronic evidence in criminal matters ("Regulation")6], and other instruments based on for judicial cooperation applicable between the judicial authorities Member States, notably those falling within the scope of under Title V, Chapter 4, such as the Directive on the European Investigation Order7 and the 2000 Mutual Legal Assistance Convention8. Recourse to the legal representative should be in accordance with the procedures set out in the instruments and legislation applicable to the judicial proceedings. The competent authorities of the Member State where the legal representative resides or is established should act in accordance with the role set out for them in the respective instrument if and where an involvement is foreseen."*

[17] The EDPB criticised the Commission's "simplified" reasoning from the data retention cases whereby everyhting that was not explicitly mentioned/prohibited by the Court the Commission considers as allowed. EDPB, Opinion 23/2018, stating (p. 14): *"In particular, the EDPB regrets that the lowest threshold providing for the possibility for law enforcement authorities to request access to subscriber and access data for any criminal offence builds on an 'a contrario' reading of the case law of the CJEU..."* See also Deutscher Richterbund, Nr. 6/18, and ECBA, Opinion o e-evidence, demanding a meaningful notification with a possible reaction in a set deadline.

data categories in existing European legislation[18] in the area of data protection and privacy of electronic communications, as well as from international treaties[19], leading to risks of mismatch and of inconsistency with the Court of Justice of the European Union's (CJEU) and European Court of Human Rights' (ECtHR) case law.[20]

[18] Article 10(2)(e) of EIO Directive 2014/41/EU, Article 4(3)(c) of the 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 (COM(2017)10).
[19] Council of Europe Convention on Cybercrime.
[20] See more WD 2 on Scope, especially as regards the issue of dynamic IP addresses.