Council of the European Union

Brussels, 30 June 2021
(OR. en)

10316/21

Interinstitutional File:
2018/0108 (COD)

LIMITE

COPEN 305
JAI 807
CYBER 194
DROIPEN 124
JAIEX 87
ENFOPOL 261
TELECOM 280
DATAPROTECT 185
EJUSTICE 70
MI 515
CODEC 1008

NOTE

From:	Presidency
To:	Delegations
Subject:	Draft Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (e-evidence) - Report on the State of Play

Delegations will find in the Annex a Report on the State of Play in the file mentioned under subject established by the Portuguese Presidency of the Council.

ANNEX

Report by the Portuguese Presidency on the state of play on the negotiations on the draft Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (e-evidence)

1. Summary

On 14 December 2020, the European Parliament adopted its report on the proposed legislative package on electronic evidence in plenary session. It therefore fell to the Portuguese Presidency to initiate the inter-institutional discussion process.

The Portuguese Presidency represented the Council in three political trilogues and in a total of 11 technical negotiation meetings with the European Parliament.

At technical level, between the first and second political trilogue, four main issues concerning the Regulation were discussed: (i) the definition of service provider, (ii) categories of data, (iii) reimbursement of costs and (iv) the common European digital exchange system.

In the first trilogue, both parties presented their positions and agreed on the working method. A broad mandate was conferred for preparatory discussions at the technical level. At the second political trilogue, discussions focused on the definition of service provider and data categories and on the topic of reimbursement of costs. Although some progress was achieved in terms of the definitions, as far as reimbursement of costs is concerned, the co-legislators' positions were, at the time, considered irreconcilable. At the request of the Commission, the discussions on the common European digital exchange system were postponed. It was decided to continue discussions at technical level on the notification mechanism, given its central role in the design of the whole system.

Under the mandate given at political level, the technical meetings thereafter focused on the notification mechanism. However, after three meetings dedicated to the topic, the Parliament insisted on also approaching other subjects of interest.

Therefore, discussions on certain aspects relating to the enforcement of preservation and production orders, languages and emergency situations were also held.

The final political trilogue took place in the Council premises on 20 May. At that meeting, representatives of both institutions reached a preliminary understanding on the lines of the Regulation concerning definitions of service providers and data categories and on those concerning the impossibility of executing a production and preservation order on formal grounds. An exchange of arguments and in-depth discussion on the notification principles took place. The mandate given to the technical level on the subject was maintained.

The COPEN Working Party was regularly informed of the work with the Parliament, through oral and written reports, and the Portuguese Presidency engaged in a continuous dialogue with the Working Party to ensure adequate defence of the general approach and a path towards a compromise solution.

The COPEN e-evidence working group meetings devoted to this package were supported by various background documents addressing the following issues: (i) the rejection of the proposed directive by the Parliament, and legal representatives, service providers covered by the regulation, data categories, reimbursement of costs and the common European digital exchange system; (ii) conditions of issue and notification; use of electronic evidence and rights of individuals; (iii) grounds for refusal and (iv) enforcement of preservation orders[1].

[1] 13525/20 INIT (08/01/2021), 5483/21 INIT (26/01/2021), 6436/21 INIT (02/03/2021), 7031/1/21 REV1 (16/03/2021), 7296/21 INIT (29/03/2021), 9291/21 INIT (02/06/2021) and WK 5973.2021 INIT (05/05/2021), WK 6504/2021 INIT (17/05/2021), WK 6945/2021 INIT (26/05/2021), WK 7451/2021 INIT (07/06/2021)

2. Latest developments

In the latest technical meetings held with the Parliament, two topics were discussed:

(i) Execution of a European Preservation Order Certificate (EPOC-PR), Article 10 of the e-evidence Regulation, lines 289 and 290 of the four-column document;

(ii) Emergency cases, namely the definition of emergency cases (Article 2(15), line 156), the ex-post validation special procedure (Article 4(5) of the general approach, line 174) and the deadline for execution (Article 8a(3) of the EP's report – line 263 and Article 9(2), line 275).

Execution of an EPOC-PR

The Council, based on the replies given by the Member States to the questions raised in WK 6945/2021 INIT, proposed the following compromise solution concerning execution of an EPOC-PR (Article 10, line 289)[2]:

1. Upon receipt of the EPOC-PR, the [addressee***/service provider***] shall, without undue delay, preserve the data requested. The preservation shall cease after ***90 days***, unless the issuing authority confirms that the subsequent request for production has been ***issued.*** [~~***The EPOC-PR can be extended by additional 30 days, where necessary to allow for the issuing of the subsequent request for production]***~~.

[2] All legal drafts included in this draft are yet to be analysed by the quality adviser and lawyer linguists.

This provision, however, had to be read jointly with a recital stating that it should suffice that the competent national authority had issued the underlying production order and that there should be no requirement for the production order to have already been translated or for all formalities such as those required in a mutual legal assistance procedure to have been fulfilled for the confirmation to be valid and the preservation time prolonged beyond 90 days:

> ***Where the requesting authority confirms within 90 days that a subsequent request for production has been issued, the service provider shall preserve the data as long as is necessary to ensure the completion and due reception of the production request. For such a confirmation to be valid and the preservation time prolonged beyond 90 days, it is sufficient that the competent national authority has issued or validated the underlying production order. It is not required that the production order has already been translated or that all formalities such as those required in a mutual legal assistance procedure have been fulfilled.***

The reasoning behind the Council's proposal was, on the one hand, to address Member States' concerns regarding the fact that 90 days would be the minimum deadline needed in more complex cases and, on the other hand, the fact that the possibility of extending the deadline in the 60 plus 30 days solution would add bureaucracy to the system, and lead to questions still to be resolved (who would extend the validity of the Order?; what process had to be undertaken to that effect?; who would determine if the 30 days were necessary?).

This proposal also had to be seen in light of the fact that, in the general approach, the procedure only had to be *launched* in 60 days, that is to say, initiated. Instead, in the 90 days, the Order has to be *issued*. The compromise text would thus mean that an Order may be considered issued already when it has *de facto* been finalised, i.e. prior to the required translation. In other words, the Order will first be issued by the competent authorities, then translated, then formally sent. The following steps, such as translation, that might be necessary for the process of e.g. mutual legal assistance, do not belong to the process of 'order being issued'. Only with this understanding of the provision were we willing to accept that it is sufficient that the issuing authority confirms it was 'issued' instead of launched (within 90 days).

The Parliament, however, did not agree with the compromise proposal put forward by the Council, expressing concerns that the order might reach the service providers without all due formalities being complied with. It also suggested that the means whereby the issuing authority confirms the subsequent request for production has been issued had to be formal (a simple email would not suffice).

Emergency cases

The Presidency initiated a discussion on the definition of an emergency situation (Article 2 of the Regulation, line 156) and on the special mechanism, introduced by the Council's general approach on Article 4(5) (line 174 of the four-column doc), according to which:

In validly established emergency cases, an Order for subscriber and access data can be issued without prior validation from a prosecutor or a judge if the validation cannot be obtained in time and if the Order could in a similar domestic case be issued without validation. The ex-post validation shall be obtained at the latest within 48 hours. Where such ex-post validation is not granted the issuing authority shall withdraw the Order immediately and shall, in accordance with its national law, either delete any data that was obtained or ensure that the data are not used as evidence.

In the last meeting, held on Friday 18 June, the discussions regarded the definition of an emergency situation and the deadline for compliance in emergency cases, which is 6 hours in the general approach and 16 hours in the Parliament's proposal. This corresponds to Article 8a(3), line 263 and Article 9(2), line 275.

The Parliament has shown openness to accepting the Council's ex-post validation of the Order mechanism, but only if the Council accepted their definition of emergency cases.

The definition of emergency cases in Article 2(15) would thus read:

> 15. 'emergency cases' means ***validly established*** situations where there is an imminent threat to life or physical integrity of a person or***, where the disruption or destruction of*** ~~to~~ a critical infrastructure as defined in Article 2(a) of Council Directive 2008/114/EC[21] ***would imply an imminent risk/threat to life, physical integrity or safety of a person.***

Article 4(5) would be subject to the alterations found below:

> **5. In validly established emergency cases, *as defined in Art. 2 (15),* the authorities mentioned under paragraphs 1(b) and 3(b) may *exceptionally* issue the respective Order for subscriber *data* and, *for the sole purpose of identifying the user, IP addresses and, where necessary, the relevant identifiers* ~~access data~~, without prior validation ~~if~~ *where* the validation cannot be obtained in time and ~~if~~ *where* these authorities could issue the Order in a similar domestic case without validation. The issuing authority shall seek validation ex-post without undue delay, at the latest within 48 hours. Where such ex-post validation is not granted, the issuing authority shall withdraw the Order immediately and shall~~, in accordance with its national law, either~~ delete any data that was obtained ~~or ensure that the data are not used as evidence~~.**

Therefore, 'emergency cases' would exclude situations where the disruption or destruction of a critical infrastructure would not necessarily imply an imminent risk/threat to the life, physical integrity or safety of a person.

The Parliament found its position to be in alignment with the definition of an emergency situation as set out under the Second Additional Protocol to the Budapest Convention. Although admitting that cooperation between Member States should be closer, the Parliament did not believe that closer cooperation changed what should be understood as an emergency situation and considered that emergency cases/urgent action are always linked to 'a (significant and) imminent risk/threat to the life (liberty) or safety/physical integrity of a (natural) person'.

The Council argued that, whereas in a convention with 66 parties it is difficult to find a common understanding of the meaning of critical infrastructures, in the EU, the common definition, as established in the Directive, provides for sufficient coherence as to the interpretation of the concept.

Besides, in the formulation as proposed by the Parliament, according to which the 'disruption or destruction of a critical infrastructure' would 'imply an imminent risk/threat to life or safety of a person', the causal link might be difficult to establish (e.g. in case of disruption of electricity is it possible to know whether a hospital has a generator and hence whether there is a risk to a person's life or not?).

In addition, some critical infrastructures, although essential for the maintenance of the State's functions, would not entail risks for a person's life or physical integrity, the example given being an attack against state-owned databases.

Finally, the weighting of the values at stake had to be considered, as on the one hand there is a need to protect critical infrastructures, the disruption of which would imply a risk of serious harm to the functioning of the state, the provision of basic supplies to the people or the safety of the people, and on the other hand the only consequence for service providers would be that they are asked to provide the data within a shorter deadline.

However, the Council's compromise proposal below was not accepted by the Parliament:

> 15. 'emergency cases' means situations where there is an imminent threat to life or physical integrity of a person or to a critical infrastructure as defined in Article 2 (a) of Council Directive 2008/114/EC ***which is essential for the maintenance of vital societal functions such as health, safety, security, and the disruption or destruction of which would imply a risk of serious harm to the functioning of the State, the provision of basic supplies to the people or the safety of the people.***

On the essential aspect of the deadline for compliance, the Council argued that the 16 hour deadline is such a prolonged deadline that the emergency situation might have passed and the damage might have already occurred. Besides, existing practice proves that urgent requests could be processed in a much shorter period of time.

The Parliament expressed concern with the difficulties that small or medium service providers would face with a shorter deadline than 16 hours.

The Council pointed to the flexibility provided for in recital 45a in the general approach, according to which the competent authorities should take into account all relevant circumstances, including the financial strength of the service provider held liable, when determining the appropriate pecuniary sanction in each individual case. Particular attention should, in this respect, be given to micro-enterprises that fail to comply with an Order in an emergency case due to lack of human resources outside normal business hours, if the data is transmitted without undue delay.

3. Final remarks

Despite the very opposing starting points of the co-legislators, a compromise text was reached on the definition of service providers and categories of data, including on the data necessary for the identification of the subject, on the grounds for non-execution of an Order for reasons of a formal nature, on the acceptance of additional languages for the transmission of Orders and certificates, as well as on the possibility that Orders may be requested by the suspect or accused person or by a lawyer representing him or her.

Even though the desired progress regarding notification has not been made, the Presidency believes that important discussions have been held to clarify and better understand the positions of the co-legislators.

During the process, the Presidency tried to ensure that the coherence of the system as a whole was never out of sight. It also advocated that, while considering the specific nature of electronic evidence, the regulation has to add value in relation to the instruments and forms of cooperation already in place, and that it should rely upon the principle of mutual trust between Member States.