Committed to Europe

Draft Regulation on cross border access to e-evidence

Summary

Due to the widespread use of electronic services and devices, criminal investigations rely more and more on access to electronic evidence, which often include a cross-border aspect. Having an efficient and secure process to speed up solving crimes thanks to access to such evidence is therefore becoming more and more crucial. A first directive on cross-border investigation was adopted in 2014 and is now at its early stage of implementation. But according to the Commission[1], the current process still shows some drawbacks as it is perceived as being too lengthy and does not cover the entire set of service providers.

To solve those issues, the Commission has adopted a new draft Regulation to ease cross border access to electronic evidence held by all types of service providers (hereafter the draft Regulation). In terms of principle, Orange fully shares the political objective of improving security and speeding up criminal investigations across the European Union. However, this should not be done to the detriment of citizens' fundamental rights and legal certainty for service providers.

The draft Regulation raises in this respect serious concerns:

- It could lead to a privatisation of law enforcement since the enforcing Member State would be deprived of any legal check, which would be done by service providers. It is paramount that national authorities remain in this process, as service providers cannot be reasonably asked to check the compliance of orders to the Charter of Fundamental Rights, verify the authenticity of the order, or its compliance with 28 criminal law systems;
- The process should guarantee the same levels of security and integrity of data transfers that the existing domestic procedures have;
- The draft Regulation should also avoid fixing rigid deadlines for answering an order and ensure that a reimbursement scheme is put in place to cover the costs on the service providers' side.

Orange has been and continues to cooperate in collecting this type of evidence with the national authorities of Member States in which we operate, seven EU Member States currently, which have implemented different regimes. Considering such experience, Orange is willing to share its operational and technical expertise to support policy makers in finding a balanced text allowing improved process without endangering citizens' rights and legal certainty.

[1] European Commission Impact Assessment; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN

October 2018

The draft Regulation should ensure more accountability for Member States increasing legal certainty for citizens and service providers

Electronic evidence is data stored in electronic form – such as IP addresses, e-mails, photos, text messages or user names – that is relevant in criminal proceedings and very often stored by service providers. It does not relate to

The fast delivery of e-evidence to judicial entities investigating crimes is of paramount importance. Considering the sensitivity of the procedure at stake, public entities should remain in charge of any legal assessment of the cross border request of accessing e-evidence. This is currently not safeguarded in the draft Regulation, on the contrary.

The draft Regulation introduces an alternative to current mechanisms imposing additional responsibilities on private entities

Today, the current procedures for gathering cross border evidence are regulated by the European Investigation Order (EIO) Directive[2] which came into force in May 2017. It replaces old procedures based on international letters of request, by the principle of mutual recognition, thereby imposing all Member States to trust each other's criminal justice, with harmonised procedures. The European Commission shall review the EIO Directive's effectiveness and present its conclusions to the European Parliament and to the Council on the 21st of May 2019.

However, according to the EC's impact assessment[3], the current procedures for obtaining e-evidence still show shortcomings, including an inefficient public-private cooperation between service providers and public authorities; the length of time to access such e-evidences; or the lack of a clear framework for service providers based in third countries. To solve them, the draft Regulation is proposing to

- Cover all types of service providers, including companies not established in the European Union; this will be done together with the adoption of the Draft Directive[4] imposing those entities to appoint a legal representative in one of the Member States for the purpose of gathering evidence in criminal proceedings;
- Create a fast track alternative to the current EIO Directive, and Mutual Legal Assistance Treaty, for the specific case of e-evidence. It creates the European Production Order (EPO) and the European Preservation Order (EPOC-PR) and allows judicial authorities of a given Member State to go directly to the legal representative of the service providers in another Member State, without any involvement of the enforcement authority of the latest.

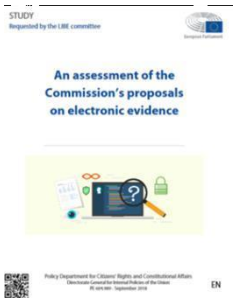
The draft Regulation is therefore imposing new obligations on service providers, which raises serious concerns in terms of preserving citizens' rights and ensuring legal certainty to service providers.

The enforcing Member State should remain in charge of the legal assessment of any EPOC or EPOC-PR (art. 9 and 14)

This is the main issue at stake with the current draft Regulation: service providers could be asked by an authority of another Member State to deliver e-evidence without any intervention of the enforcing Member State, where the EPOC or the EPOC-PR is executed. This means that service providers would be asked to assess whether an order is compliant with the criminal laws of the Member States concerned and with the Charter of fundamental Rights of the EU.

[2] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.
[3] See footnote 1
[4] See https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN

This cannot be the case. Service providers are neither legitimate nor competent to assess such compliance; they should be asked to simply answer an order. The enforcing Member State should remain in charge of the compliancy test with all types of law. This is the only way to preserve citizens' rights and grant legal certainty to service providers.



This provision is also highly criticised in the assessment of the Commission's proposals on electronic evidence, made for the European Parliament that concludes[5]:

> "As a consequence, the "executing" MS does not assess whether the conditions for execution are met, and the individual is deprived of a control mechanism aimed at the protection of his/her fundamental rights."

Articles 9§5 and 14§4 and §5 should therefore be substantially reviewed. Finally, the non-liability clause mentioned in recital 46 should be included in an article to reinforce legal certainty for service providers.

The draft Regulation should also be modified on other aspects to guarantee the efficiency of the procedures

The draft Regulation should take more into account the use of existing mechanisms to achieve its objectives while ensuring the feasibility of its provisions.

Existing national platforms or mechanisms ensuring secured communication channels should not be circumvented (art.8)

Article 8 states that the EPOC and EPOC-PR shall be directly sent to the service provider and that the use of secure channels is optional for the issuing authorities.

As explained above, Orange considers that the enforcement authority should be the entity that receives the EPOC or EPOC-PR, and then forwards it to the service provider. Each Member State should establish one single point of contact entitled to exchange information with its EU counterpart. Some countries have already created centralised platforms, such as in France, Romania or Spain[6] to name a few. Such platforms should not be circumvented or rendered useless by the draft Regulation; on the contrary, they should remain at the heart of the process. Without this, each issuing authority in a given Member State will face "n" service providers, with "n" different ways to be addressed and to exchange electronic evidence.

In relation to the means used to transmit the request and the disclosed data, the usage of secure channels should be mandatory to grant the confidentiality of the investigations and of the concerned individuals. Doing otherwise would create a high risk of downgrading current information exchanges, such as, current security certified channels versus for instance possible fax transmissions.

[5] http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2018)604989

[6] For France, Romania or Spain, see the PNIJ Plate-forme Nationale d'Interceptions Judiciaires, Serviciul Roman de Informatii (SRI), Sistema Integrado de Interceptación Telefónica (SITEL).

The draft Regulation should not fix rigid deadlines (art. 9)

Article 9 of the draft Regulation sets concrete deadlines to disclose the data requested: 10 days for requests and 6 hours for urgent requests. Orange believes that those detailed deadlines should be deleted and replaced respectively by "due diligence" and "without delay". Today, many countries do not set a deadline, however, some of them distinguish between urgent and non-urgent requests. They rely on the service provider to act immediately, with urgent requests being prioritised over others.

This avoids putting the service provider in a difficult or even impossible situation of having to choose which request might be more urgent than another. It also does not raise any specific difficulty; as far as Orange is concerned, we have not been subject to complaints on the time taken to answer orders.

Fixing a deadline at EU level for a cross border request would have negative side effects. For instance, regarding domestic requests without a legal deadline, should the service provider prioritise the European urgent request with a 6 hour deadline? The requests should be managed distinguishing between urgent and non urgent, no matter whether they are domestic or cross-border.

The draft Regulation should provide for a fair compensation of costs based on the enforcing Member State law (art. 12)

The draft Regulation will lead to an increase of requests coming from various Member States, which will require additional investments and maintenance costs. Some Member States have already foreseen in their national law such reimbursements, for instance in France[7], Germany or Belgium. The draft Regulation should include a reimbursement scheme for both investments and operational costs, covering also those countries that don't have this type of scheme recognised in their national laws yet.

For more information: https://oran.ge/in-Brussels , or follow us on Twitter: @Orange_Brussels

[7] See for instance French « Arrêté du 12 janvier 2018 ». https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000036496527&dateTexte=20180715