CEPIS | CELEBRATING 30 YEARS

LIBE Committee Members

Brussels, 17 December 2019

E-evidence Regulation: No direct cross-border access to personal data

Dear Members of the European Parliament,

As MEPs, you are participating in the debate on the European Commission's proposal for a Regulation on cross-border access to electronic evidence in criminal matters. We are approaching you to express our concern about the proposal.

The draft includes enabling law enforcement authorities of a Member State (issuing state) to directly oblige providers established in another Member State (enforcing state) to disclose metadata and content data of their customers. The disclosure must take place within ten days and, in emergencies, within six hours. If providers fail to do so, they could face sanctions of up to 2% of their worldwide annual turnover. The enforcing state is not obliged to review the order for legality and has no right to object to it. On the other hand, it is obliged to impose and enforce a sanction against the provider in the event of non-compliance. The offence under investigation does not necessarily need to be a criminal offence in both states (dual criminality). Providers based in third countries, in which the offence under investigation is not a criminal offence, would also be obliged to disclose data if they offered services in the European Union.

We strongly warn against this initiative. The proposal deprives states of the ability to protect the fundamental rights of their citizens. It undermines European data protection law and threatens to damage the existing international system of mutual legal assistance in criminal matters. Only two years after the deadline for implementing the European investigation order, it has not been clarified whether there are any gaps in cross-border criminal prosecution.

Please find our points of objection in detail as an attachment to this letter.

Yours sincerely,

Byron Nicolaides
President

CEPIS CELEBRATING 30 YEARS

Our points of criticism in detail:

Protection of fundamental rights cannot be guaranteed
The enforcing state has no possibility of ensuring compliance with fundamental rights
(1) The cases in which data may be disclosed shall be governed exclusively by the law of the issuing state. This makes it possible for investigating authorities from other European countries to receive data from a country under lower thresholds than would be possible for that country's authorities. This may also mean undermining the provisions of the Code of Criminal Procedure or constitutional rights in that country.
(2) The enforcing state cannot guarantee the protection of professional secrets, immunities and rights to refuse to give evidence or the proportionality of data processing. The notification procedure added by the European Council does not constitute a sufficient means of protection, since the enforcing State can only provide indications that immunities or holders of professional secrets are affected but has no right to a binding refusal.

Political persecution is possible without dual criminality
Criminal law is not harmonised in the Member States of the European Union. What is considered a criminal offence and what is not is very different. For example, the penal laws on abortions range from a comprehensive ban to extensive liberalisation. In some countries it is a crime to attribute the population or state a share of responsibility for specific crimes against humanity. There are also considerable differences with regard to the violation of banking secrecy and many other offences, sometimes involving local politicians. E-Evidence forces providers and states to participate in the prosecution of acts that are legal in their country. This will also lead to politically unwanted results.

The necessity of the instrument is not proven
Only in 2014 the European Parliament adopted the Directive on the European Investigation Order, which is intended to enable faster cooperation between law enforcement authorities. It creates binding deadlines for cross-border cooperation. The deadline for implementation did not expire until 2017. An evaluation has not yet taken place. There are no studies on what the European investigation order contributes to obtaining electronic evidence, whether there is need for improvement and where possible weaknesses lie. There is also a lack of information on the number of cases in which investigations had to be discontinued because access to electronic data was not possible. Without knowledge about the effectiveness of recently established instruments, the introduction of a new set of rules is disproportionate. We call for an evidence-based policy.

We fear an international spill-over effect which will ease political persecution.
International cooperation in criminal matters has so far been characterised by mutual legal assistance. The E-Evidence regulation also affects services based in third countries that store data outside the EU. If the EU unilaterally establishes rules that are to apply in other states, it breaks with the concept of mutual legal assistance. This will invite third countries to proceed in a similar way. Authoritarian states can also oblige international providers to release data stored in the European Union. This endangers politically persecuted persons seeking protection abroad.
In addition, principles of the GDPR are being undermined: GDPR requires data processors to transfer data stored in the EU to third countries only under very strict conditions. The E-Evidence proposal, however, does not consider whether national data protection laws of third countries permit a transfer to the EU.

The European Commission's negotiations with the United States, which have already begun, are bypassing the Parliament.
The European Commission has already started negotiations with the USA on an administrative agreement before the European Parliament has been able to form an opinion on the E-Evidence on which this agreement will be based. This start of negotiations not only neglects the European Parliament as the directly democratically legitimised institution of the EU. The US have already laid down the framework for such an agreement in a law passed in 2018, the CLOUD Act. Much speaks for the impossibility of an agreement that

meets the requirements of both the GDPR and the CLOUD Act.