EUROPEAN LAW BLOG
NEWS AND COMMENTS ON EU LAW

ELB Blogpost 37/2022, 20 September 2022
Tags: European criminal law, criminal investigation, enforcement, internet service providers, private actors, mutual recognition, European Production Order
Topics: Criminal proceedings, Data protection and digital governance, Fundamental rights, Mutual recognition

The public role of private actors: Internet service providers in the E-Evidence proposal

By Stanislaw Tosza

The European Commission proposed on 17 April 2018 the "E-Evidence" legislative package (E-Evidence) to overcome the widely discussed issues relating to the traditional instruments for cross-border gathering of electronic evidence (K. Ligeti, G. Robinson; S. Tosza 2020). The main innovation of this proposal consist in allowing law enforcement in one member state to directly compel service providers in another member state to produce or preserve data (for a comprehensive analysis of the proposed package, see V. Franssen in this blog). Already now Internet service providers (ISPs) play a key role of gatekeepers to the data they have, especially in the context of voluntary cooperation. Because of limited possibilities for enforcement, the often transnational context of data gathering and economic power of major ISPs, they are the ones to decide whether to provide data to authorities or not (I develop this argument in details here). While the final text of the EPO Regulation is still being negotiated, in this post I argue that the proposal for the E-Evidence regulation (in all its available versions) does not solve the problem of such "privatisation" of enforcement in the context of e-evidence gathering (V. Mitsilegas) and explain why this is worrisome.

E-Evidence legislative package – difficult negotiations

The E-Evidence proposal has been in the legislative pipeline for a while already. While the EU Council adopted its general approach fairly quickly, on 7 December 2018 (for its analysis see T. Christakis), the European Parliament's (EP) lengthy discussions took almost two years. The EP presented its Report on the draft Regulation finally on 11 November

2020 and it differed significantly on several points from the relatively similar to the Commission's proposal general approach of the Council (see also T. Christakis in this blog).

The interinstitutional dialogue that followed started in February 2021, but quickly stalled, with the main contentious point being the notification requirement. The original proposal of the Commission implied that the authorities in one Member State address directly an ISP in another Member State, while the authorities of the latter state remain unaware of that request (and, inevitably, without a formal say on it) unless the ISP refuses to cooperate. Only then they can come into play. This approach was questioned by the Council and to a larger extent by the Parliament. Both introduced the requirement that the Member State of the ISP to which the request is addressed be notified about the request: in limited cases (Council's general approach, Art. 7a) or always (Parliament's position), but with different effects depending on the type of requested data (see below for details). While the Parliament seemed to insist on its approach in the trialogue negotiations, the Council seemed to disagree. A recent communication signals, however, that an agreement between the co-legislators on that issue has been reached, although its details are not yet known.

Public role of ISPs in e-evidence gathering

According to the E-Evidence proposal, ISPs may refuse complying with the EPO on a limited number of grounds. This *numerus clausus* differs in the three versions of the Regulation. These grounds belong to two major categories: (i) reasons related to the form or conditions of issuing of the order: it has not been issued or validated by the competent authority; it has been issued for offences to which it was not applicable; the service is not covered by the Regulation; (ii) *force majeure* or *de facto* impossibility of the ISP: the person whose data is sought is not their customer, or the data has been deleted before receiving the EPdO. The Commission proposal provided for an additional reason for refusing the order: a manifest violation of the Charter's fundamental rights or the manifest abusiveness of the order (Article 9 (5) of the Commission's Proposal), a refusal ground, which is notably deleted in the Council's General Approach . The EP's included the possibility for the ISP to refuse the execution of the order when it is manifestly abusive or when it exceeds the purpose of the order (Articles 9 (5) and 10(6) of the EP's Report).

Depending on the formulation of grounds for refusal, the responsibilities placed on ISPs may be wider or narrower. However, regardless of whether the possibility for ISPs to reject abusive orders is enshrined in the Regulation or not, the ISPs may find themselves compelled – for different reasons – to refuse abusive orders. For instance, requests might concern data for offences which are not subject to criminalisation in the state of their main operation and where public opinion might be more leaning against such criminalisation (e.g., abortion). They might be pressured to resist such orders by the civil society, including

NGOs, politicians and even by the government of the state in which they reside (S. Tosza 2019). In effect, ISPs have to perform value judgments weighting different interests at stake, a decision more similar to what a judge should be doing when deciding on the access to data (and allowing the resulting limitation of the right to privacy).

Additionally, these value judgments have to be carried out under the pressure of punitive sanctions, although the details (and effectiveness) of this framework remains an open question as they ought to be provided at the national level (Article 13). Given the economic clout of the major providers, it is likely that they will not deter them from refusing the order, if they consider it necessary as it happened in some notable cases (*Yahoo*, *Skype*, *FBI vs Apple*). Eventually, ISPs will take their decisions according to their economic or reputational interests, and the possibility of receiving a fine will be calculated together with other factors.

In any case, it is no surprise that one of the major ISPs favours including the possibility for them to effectively challenge 'an unlawful or otherwise inappropriate demands for user data' (L. Cosette). However, the need to address this problem does not stem from the need to provide a comfortable framework to the ISPs. It is part of a more fundamental question about the execution of public power and the private actors' role in protecting fundamental rights.

Limited impact of the notification requirement

The EP's position which adds the mandatory notification system is an attempt to limit the "privatisation" of enforcement, i.e. reallocating the duty to assess the existence of grounds for refusal to the competent authority of the executing member state. In that proposal, when an EPO is issued for obtaining traffic or content data, the ISP should refrain from executing the request until the time limit for the judicial authority of the executing member state to review the order elapses. The time limit is of 10 days for a normal request and 16h in case of urgency. The regime proposed by the EP has a suspensive effect, but the silence of the competent authority means no objection. Only for requests for traffic or content data coming from states subject to the procedure referred to in Article 7(1) or 7(2) of the TFEU, the ISP cannot transmit the requested data until it receives explicit written approval from the competent authority of the executing member state (Article 9(2a) EP's Report).

At this point the details of the agreement within the trialogue on the notification requirement are not known. While these details are important, in any case the notification will not deprive the ISPs of their controlling function at least for three reasons. First of all, it is possible that notifications will be just a bureaucratic duty as many Member States might not be willing to allocate personnel to analyse requests and potentially refuse them. Secondly, the question which country plays the role of the executing member state

depends on the location of the ISP and is not connected to the question of the nationality or residency of the person whose data is sought. This means that the executing member state has limited interest in verifying such order. Finally, even if the executing member state confirms the order, ISPs might still *in casu* be willing to refuse it, for instance for reasons mentioned above. In consequence, the notification might not fundamentally change the position the ISPs play in the system of producing data to serve as evidence in criminal investigations and trials.

Conflicting roles of private actors

In view of the above, irrespective of the introduction of the mandatory notification system, the E-Evidence package will create a new relationship between law enforcement offices and ISPs. These are likely to "become extended arms of law enforcement replacing their national authorities in the task of not only receiving and complying with but also assessing the orders". ISPs will become, inevitably, more of a public authority than a private actor, not having, however, all those features that characterise public authorities, namely: accountability, impartiality and independence

This transfer of public responsibilities to ISPs, proposed by the E-Evidence package, is not new in European legislation, but rather fits into a trend that has been amplifying in recent years (M. de Cock Buning, L. Senden). Indeed, private actors have been more and more involved in crime prevention. The AML regulatory framework constitutes a paramount example of this trend: private actors, in particular banks and financial institutions, are obliged to design risk prevention rules and to report to competent authorities in order to prevent money laundering or terrorism financing. In that sense, the E-Evidence proposal codifies a quantum leap in the role of private actors: they are not only involved in crime prevention, but are required to play an active (proactive) role in enforcement, by directly answering requests from a law enforcement authority and evaluating, *prima facie*, the validity and legitimacy of these requests (S. Tosza 2020).

This role raises numerous questions. ISPs, as private actors, are profit-driven entities that are accountable to their owners or stakeholders. These characteristics have a (at least) two-fold impact on their capacity of fitting this public role. Firstly, ISPs will take decisions according to their business interests. Indeed, when they have to make choices between conflicting values, unlike the public actors, ISPs perform this role while risking sanctions for non compliance or reputation consequences, which may directly affect their business interests. Moreover, even if private actors may present themselves as acting for a greater good, they will behave in such a way only as long as this is aligned with their business interest. Secondly, the business logic affects ISPs accountability and responsibility. A democratic system of accountability provides controls of value judgments in a public

sphere (M. Bovens); private companies (i.e. the ISPs) are foremost accountable to their owners.

Lastly, more practical problems related to the execution of such power may appear related to possible misuse of ISPs powers. For example, what about corruption proposals made to individual employees regarding ISPs decisions which they perform? This type of corruption, however, does not regard anymore the private sphere, as it is not a breach of the duties towards the entity. This situation would be more similar to public corruption, but is not covered by the respective regulations. (S. Tosza 2021)

Concluding remarks

Cooperation between law enforcement authorities and ISPs appears to be necessary, as the latter have at their disposal information that may be vital for the conduct of criminal investigations. The actual regulatory framework is not adapted for governing this new relationship between public authorities and private actors. Hence, a legislative intervention is necessary, and the E-Evidence package has the potential of solving one of the key obstacles for modern criminal investigations. However, there should be a more comprehensive framework assuring that the rights of the affected persons can be sufficiently safeguarded and that their fate is not dependent on the business interest of private companies.

The problem of the public role of ISPs is not limited to gathering e-evidence. Similar problems and arguments can be made in the context of the online content regulation and the debate around the Digital Services Act (DSA, I analyse this issue in details here). The difficulties in negotiating both legislative initiatives (E-Evidence and DSA) demonstrate how challenging it is to regulate a sphere where private actors have so much effective enforcement capacity and *de facto* adjudicative power. Yet, a clear set of boundaries is necessary in order to assure the fairness of the proceedings and the correct protection of the fundamental rights of the affected persons. If such a *shared adjudication* has to be accepted, a much more enhanced framework needs to be provided that assures that the rights of the affected persons.