EU legislation on e-evidence – what is inside the (Pandora's) box?

Summary by Alessandra Calvi (VUB/LSTS) and Juraj Sajfert (VUB/University of Luxembourg)

On 21 April 2021, the Brussels Privacy Hub, in cooperation with the **University of Luxembourg** within the framework of the FWO/FNR-funded MATIS project, and in media partnership with **Privacy Laws & Business** organised the fourth webinar within the series **Enforcing Europe - Webinar Series 1,** .

The fourth webinar, entitled **EU legislation on e-evidence – what is inside the (Pandora's) box?** discussed the EU upcoming legislation on access to electronic evidence - encompassing a proposal for a Regulation on European Production[1] and Preservation[2] Orders for electronic evidence in criminal matter and for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings - currently in trilogues.

The idea behind this legislative reform is to enable the law enforcement authorities to compel online service providers into surrendering the personal data of their customers, even if the service providers are based outside of their jurisdiction. The law enforcement's reach to service providers will therefore become direct, without the traditional channels of law enforcement cooperation such as mutual legal assistance (MLA) or mutual recognition. Is this a necessity in the digital era, or a game-changer with unforeseen consequences for the basic principles of both criminal procedural law and data protection law?

Juraj Sajfert (VUB/University of Luxembourg) moderated the discussion. Invited speakers were **Anže Erbežnik** (European Parliament, LIBE committee secretariat), **Marco Stefan** (Centre for European Policy Studies), **Luc De Houwer** (Belgian Federal Prosecutor's Office) and **Elisa Sason** (Dutch Permanent Representation to the EU) who tackled the following questions:

- *What are the main issues on the table?*
- *Where are the big differences between the Parliament's and the Council's position?*
- *What could be the possible compromises, and how will they shift the paradigm as we know it?*
- *What about the other pieces of the e-evidence puzzle - the reform of the Cybercrime Convention, US Cloud Act and the potential EU-US agreement?*

The speakers spoke in their personal capacity.

Anže Erbežnik provided insights as to the state of play of the legislative proposals in the trialogue. The Council agreed its position on the proposal for a Regulation on cross border access to e-evidence in December 2018, whereas the European Parliament adopted its position in December 2020. The trilogue started in February and another one will take place in May. He noted how the two positions substantially differ in terms of:

[1] "The European Production Order will allow a judicial authority in one Member State to request access to electronic evidence (such as emails, text or messages in apps) directly from a service provider's legal representative in another Member State, which will be obliged to respond within 10 days, and within 6 hours in cases of emergency (as compared to 120 days for the existing European Investigation Order or 10 months for a Mutual Legal Assistance procedure)."
https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345

[2] "The European Preservation Order will allow judicial authorities in one Member State to oblige a service provider or its legal representative in another EU country to prevent electronic evidence from being deleted before their production request is completed. The orders will apply only to stored data. Real-time interception of telecommunications is not covered by this proposal."
https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345

- Rules on notification of the European Production Order: for the EU Parliament, the executing State's authority may refuse the execution of a European Production Order based on specific grounds for non-recognition or non-execution.
- Definition of 'cross-border situation': for the EU Parliament the definition of a cross-border situation depends on where the data controller is.
- Procedure to apply in case of manifest democratic deficiencies: for the EU Parliament, if an order comes from a Member State undergoing a procedure under Article 7 TEU, data may only be released after explicit confirmation by the executing State.
- Categories of data: whereas the Commission and the Council enumerate four categories (i.e. subscriber information, access data, traffic data and content), the EU Parliament considers only three, namely subscriber, traffic and content.
- Relations with ePrivacy and challenges posed by modern technologies: for the EU Parliament, greater coordination between the two instruments is needed.

He referred to the landmark judgement Bivolaru and Moldovan v. France (Application Nos. 40324/16 and 12623/17) issued by the European Court of Human Rights to emphasise that still nowadays European Countries lack common standards in criminal matters (e.g. right to access to a lawyer).

Marco Stefan, referring to the October 2020 report issued by the Centre for European Policy Studies (CEPS) and the Queen Mary University of London (QMUL) Task Force, illustrated the major criticalities of the e-evidence framework. He observed that the impact assessment of the Commission did not fully demonstrate the necessity and proportionality of the proposal. The mere increase of the number of requests of European Investigation Orders is insufficient to justify the circumvention of the guarantees posed by the reciprocal judicial scrutiny of cross border data-gathering measures. He argued that the e-evidence proposal will be a game-changer because the direct access to e-evidence will compromise, *inter alia*, the secrecy obligations of journalists, doctors and lawyers and the right to an effective remedy that EU law grants to suspects and accused persons, as well as legal certainty and sovereign prerogatives of states.

Luc De Houwer noted that practitioners need an instrument suitable to allow them to follow the changing times. Albeit, currently, it is not possible to evaluate which of the two proposals would be the best. The first impression is that the European Production/Preservation Order system proposed by the EP is not user-friendly and leaves a lot of power in the hand of private companies, whereas judicial authorities remain accountable, the proposed system of notification by the EP is not at all userfriendly. He pinpointed also issues in terms of privileges and immunities, admissibility of proofs and competent authorities allowed to issue it. He noted that prosecutors and judges when performing an investigation and searching for proof, always act in respect of procedural law, as well as EU law, including the Charter of Fundamental Rights of the European Union. Investigations lead by competent judicial authorities are always "a charge and a decharge".
He noted that the rights of victims are very important and often forgotten, and cross border investigation should be made from the moment victim's rights need to be ensured following the jurisprudence of the Court of Justice. He admitted that the European Production/Preservation Order could be a game-changer, but not the best system of obtaining IP- identifications, if the proposed system will be more demanding then the EIO system or national systems.
He added that MLAs (outside the EU) were working well for some types of data and that the Budapest convention system, as well as voluntary cooperation, will remain in place.

Elisa Sason stated that the Netherlands has been a strong supporter of the exchange of e-evidence. She emphasised that the Netherlands did not support the Council general approach together with other 7 Member States. She identified three key aspects of the upcoming legislative framework:

- Role of Internet Service Providers. She noted that the Commission proposal adopted an entirely new approach by putting Internet Service Providers at the same level as the issuing

States. She noted that the EU Parliament has proposed to integrate into the regulation many provisions of the directive, including for the reason not to overburden SMEs. Whereas this could enhance legal certainty, it may be a problem in terms of the legal basis to adopt EU legislation in relation to this file.

- Notification procedure. The Council general approach provides for notification to the executing State, yet only for content data and only if the issuing authority has grounds to believe that the person does not reside in its own territory. The Netherlands argued that more guarantees are needed and also pleaded for a stronger role of the executing authority. Nevertheless, the position of the EU Parliament requiring notifications for all types of data categories may go a bit too far. She argued that the most sensitive data categories - content data and traffic data – should be subject to a meaningful notification procedure.
- Grounds for refusal. She argued that there should be sufficient grounds for refusal, including e.g. *ne bis in idem*, fundamental rights and double criminality. She argued that the EU Parliament included a lot of grounds for refusal, whereas the best solution would be a middle ground between the position of the Council and Parliament.

During the Q&A, Anže Erbežnik highlighted that more and more cases have a cross-border element, and e-evidence will be the main legislation on cross-border cooperation. Referring to La Quadrature du Net judgement, he noted that when procedures are rushed, they lead to bad results. He expressed concerns on the lack of standards on the admissibility of e-evidence and on the duty given to private companies to make fundamental rights assessments.
Luc De Houwer argued that the increase of cybercrime does necessarily entail an increase in cross-border cooperation. He added that investigations are not just about access to data, e.g. EIO and MLA provide in the possibility to hear witnesses and victims in another country by videoconference.
Marco Stefan insisted on the importance of creating EU standards to increase trust, as direct access does not have a lot to do with judicial cooperation. He insisted on the importance of maintaining mutual recognition in the EU and third countries.
Elisa Sason argued that digital evidence is needed in almost all investigations and that direct access to it represents an added value compared with the system of the European Investigation Order. She argued that the debate on data retention is something separate.