Guest editorial eucrim 2-2023

Birgit Sippel

eucrim
European Law Forum: Prevention • Investigation • Prosecution

EDITORIAL

AUTHOR

Birgit Sippel

Member of the European Parliament (S&D)
European Parliament

CITE THIS ARTICLE

Sippel, B. (2023). Guest editorial eucrim 2-2023. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2023-011

Published in eucrim 2023, Vol. 18(2) p 109

https://eucrim.eu

ISSN:

Dear Readers,

On 12 July 2023, after more than five years of, in part, very fraught negotiations, the European Parliament and the Council signed the so-called “e-evidence package”. This marked the turning point in the cooperation between law enforcement authorities and service providers. Criminal offences prepared and carried out exclusively offline are a thing of the past, which is why electronic evidence is becoming increasingly important for law enforcement authorities. However, e-evidence is frequently stored in another State and, until now, cross-border access to such evidence was often very burdensome, often resulting in possibly already getting lost and causing investigations to be stopped inconclusively. The new EU internal rules will now allow national authorities to request evidence directly from service providers in other Member States or to ask that data be preserved, based on EU-wide harmonised rules and deadlines.

Driven by the singular objective of speeding up the process, however, the initial Commission proposals and partly also the Council position completely ignored the fact that criminal law across the EU is far from being fully harmonised, beginning with the question of what constitutes a (serious) crime. The drafters of the new Regulation and Directive also turned a blind eye to the fact that the rule of law and the protection of fundamental rights is not a given, not even within the EU. In my capacity as Parliament Rapporteur for the package, I have therefore done my utmost to ensure that cross-border judicial and police cooperation were adapted to today’s digital reality, on the one hand, and, on the other, that fundamental rights (in particular the rights to privacy and to the protection of personal data) remain protected and procedural safeguards are ensured .

As representatives of the European Parliament, we successfully pushed for the introduction of a notification regime: When it comes to production orders for the most sensitive data categories – traffic and content data –, the State in which the service provider is addressed will (barring exceptions) have to be notified about the order. The notified authorities will then have ten days to refuse the order, based on a clear list of grounds, including concerns about media freedom and fundamental rights violations in the requesting Member State. Parliament also made sure that service providers will be able to flag concerns. Furthermore, we pushed through the introduction of a decentralised IT system, in order to ensure that orders and data are safely exchanged as well as to guarantee that service providers receive orders only from authenticated authorities.

The years leading up to the signature of the package have been a political rollercoaster, with the European Parliament and the Council initially defending quite different positions. Personally, I would have preferred an even broader notification regime, additionally covering the ostensibly less sensitive data categories (i.e. subscriber data and IP addresses); however, this was impossible due to strong opposition from the Member States and even the conservatives in the Parliament. In the end, both sides had to compromise.

Now, the time has come for this package to be thoroughly implemented, so that it can deliver the goods we have been aiming for. The role of the European Parliament and my role as Rapporteur does not stop here. Quite the contrary! The internal rules lay only the groundwork for future international cooperation agreements. On behalf of the EU, the Commission is negotiating both a potential EU-US e-evidence agreement and a UN convention on cybercrime. As Rapporteur for the EU-US negotiations and shadow rapporteur for the UN convention, my colleagues and I will keep a very close eye on all further developments. Because one thing is clear: The protection of fundamental rights, in particular the right to privacy and the protection of one’s data, is a whole new ball game beyond the EU!

https://doi.org/10.30709/eucrim-2023-011

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and “criministrative” law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU’s financial interests – a key driver of European integration in “criministrative” justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union