Fast-Tracking Law Enforcement at the Expense of Fundamental Rights

Valerie Albus 2023-06-15T15:47:36

Five years in the making, the EU's e-evidence Regulation was finally adopted by the European Parliament on June 13. The Regulation will allow law enforcement authorities to directly compel online service providers operating in the EU to preserve or produce e-evidence in the context of criminal proceedings. This is achieved through applying the principle of mutual recognition to cooperation with online service providers, thereby skipping judicial control in the Member State where the service provider is established. Whilst these innovations have been lauded for facilitating access to data in cross-border cases, this blogpost will detail how the Regulation's emphasis on speed and efficiency comes at the expense of safeguarding suspects' fundamental rights. The following legal analysis is based on the final text published by the Council in January.

An EU-wide Duty of Cooperation for Online Service Providers

The e-evidence Regulation promises to facilitate and speed up the process of obtaining e-evidence from online service providers – such as Google or Meta – in cross-border cases. It defines e-evidence as subscriber data, traffic data, or content data stored by an online service provider in electronic form. Cross-border cases, meanwhile, are those in which the service provider is established or represented in a different Member State than the law enforcement authorities issuing the order. According to the European Commission, these cross-border situations represent more than half of all requests for cooperation in the EU.

Prior to the reform, law enforcement authorities had to request assistance from the Member State in which the service provider is established, relying on mutual legal assistance instruments or the European Investigation Order. The main innovation of the e-evidence Regulation is to create a channel for *direct cooperation* with online service providers, regardless of their Member State of establishment or the location of the data. It does so by creating two new binding instruments: the European Preservation Order and European Production Order. Whilst the former allows law enforcement authorities to request the preservation of data for the duration of 60 days, the latter allows them to compel service providers to produce data within 10 days. Due to limited space, the present analysis will mainly focus on the European Production Order, as it is the more intrusive instrument.

Expanding Mutual Recognition to Private Actors

Direct cooperation with online service providers fundamentally changes the architecture underlying criminal law cooperation in the EU. After all, cooperation has traditionally taken place between judicial authorities and relies on the principle of mutual recognition. The idea underlying mutual recognition is simple: a judicial authority in Member State A may issue an order which will then be recognised and executed by a judicial authority in Member State B. Mutual recognition instruments account for most cooperation instruments in the area of criminal law, such as the European Arrest Warrant, the abovementioned European Investigation Order, or freezing and confiscation orders.

The e-evidence Regulation also relies on the mutual recognition mechanism and thereby marks the first application of this principle to cooperation with private actors (for an in-depth analysis of this, see Tosza 2019). This has important procedural consequences: instead of sending a cooperation request to a judicial authority in another Member State and awaiting the recognition and execution decision by a judge, a European Production Order can be addressed directly to the service provider. Service providers must then process and give effect to the order within 10 days or, in emergency cases, within 8 hours. Non-compliance may lead to the imposition of sanctions of up to 2% of the total worldwide annual turnover of the service provider's preceding financial year.

More Speed, Fewer Safeguards?

Whilst these modalities undoubtedly reduce the time it takes for law enforcement authorities to obtain access to e-evidence, they also dispense with a crucial layer of control. Whereas the suspect could previously rely on the assessment of two judicial authorities – the first one issuing the order based on its national law and the second one ensuring that the order does not violate fundamental rights or fundamental principles of criminal law – the e-evidence Regulation effectively skips this second assessment.

This is remarkable given that the CJEU has repeatedly emphasised the importance of this second assessment in cases concerning criminal law cooperation. For example, in the context of the European Arrest Warrant, the Court held that there is an obligation to refuse cooperation where there is reason to believe that this would lead to the violation of a fundamental right, such as the prohibition of inhuman treatment (*cf.* Joined Cases C-404/15 and C-659/15 *Aranyosi and C#ld#raru*) or the right to a fair trial (*cf.* Case 216/18 *LM*). Of course, these cases concern the surrender of persons and do not apply in the same manner to data-sharing. Yet, this should not blind us to the fact that data-sharing is a practice rife with fundamental rights concerns. As the association European Digital Rights (EDRi) points out, there is a significant risk that the e-evidence Regulation will lead to a general increase in surveillance, or might get abused to target journalists, activists, and political opponents. These risks, they emphasize, are especially serious for individuals residing in Member States with systemic rule of law deficiencies.

Whereas previously, they could rely on messaging services based in other countries to protect the privacy of their correspondence, the e-evidence Regulation leaves them especially vulnerable to abusive European Production Orders.

Who Guards the Suspect's Fundamental Rights?

The proposal of the e-evidence Regulation included a fundamental rights-based ground for refusal which the online service provider could invoke if the execution of a European Production Order would amount to a manifest violation of the Charter of Fundamental Rights. This provision was deleted by the Council during trilogue negotiations. Giving online service providers the possibility of refusing to execute a European Production Order by no means seemed like a failproof way of ensuring respect for fundamental rights. Among other things, this provision was criticised for overburdening smaller service providers that may not necessarily have the infrastructure or a team of lawyers to assess whether a request for cooperation complies with fundamental rights law. It was also pointed out that leaving fundamental rights control to the service providers would effectively lead to a privatisation of law enforcement (for a critical overview of the e-evidence proposal see Franssen 2018).

Instead, the final text of the Regulation creates a notification requirement that aims to bring the burden of the fundamental rights control back to the state. For European Production Orders issued to obtain traffic or content data a copy of the order should be transmitted to a 'competent authority' in the Member State where the service provider is established. The Regulation leaves it to the law of the Member States to determine who this authority is and does not expressly require them to be a judicial authority. The competent authority then has 10 days or, in emergency cases, only 4 days to raise a ground for refusal.

The Result: Serious Fundamental Rights Concerns Remain

However, even with a notification requirement, the fact remains that henceforth the logic underlying cooperation requests will be reversed: instead of a judicial authority actively taking a decision on the recognition and execution of an order emanating from another Member State, automatic execution is now the rule, except where the competent authority chooses to intervene and raise a ground for refusal. This arrangement is fundamentally at odds with meaningful judicial oversight which is key to safeguarding fundamental rights in the context of extraterritorial enforcement of criminal law.

Moreover, practical considerations raise doubts as to whether the notification requirement will be suited to uphold a high and uniform level of fundamental rights protection in practice. Firstly, the person whose data is being sought might not necessarily be a national of the Member State that gets notified, and this might reduce the incentive of the competent authority to oppose the request. Secondly, the workload between the different competent authorities is bound to differ significantly.

For example, it is likely that the designated authority in Ireland, which hosts most European headquarters of Big Tech companies and has expressed its intention to take part in the application of the Regulation, will receive a comparatively high number of notifications. In light of the short time limits and the fact that many EU Member States – including Ireland – are already struggling with overburdened justice systems, it is unclear whether this notification requirement can provide an effective layer of protection. Finally, the fact that requests for subscriber and traffic data obtained for the sole purpose of identifying the user are excluded from the notification requirement does not exactly lessen concerns over surveillance.

In conclusion, the modalities of the e-evidence Regulation make it plain that the instrument was designed primarily with the interest of law enforcement authorities in mind. It is doubtful whether the purported advantages of direct cooperation will outweigh the risks of abuse and fundamental rights violations – but evidently, this is a price that the EU legislator was willing to pay.
