e-Evidence compromise blows a hole in fundamental rights safeguards

In December 2022, the Council and the European Parliament agreed on a final compromise text on the so-called 'e-Evidence' proposals. With major concessions given to the Member States' position, the results of these trilogues negotiations are of bad omen for people's rights and freedoms.

By **EDRi** - February 7, 2023

What's the aim of the e-Evidence proposals?

Initiated by the European Commission in 2018, the 'e-Evidence' Regulation and Directive aim to 'ease' access by law enforcement authorities to personal data held by private online service providers established in other Member States. The basic idea behind this proposal is to allow investigative authorities to send requests directly to companies, whereas the current rules of judicial cooperation require them to ask their counterparts in the country where the company is established for assistance in getting the data. In simpler terms, **the objective is to cut short current judicial processes**.

This model of "direct requests" was criticised at length by numerous stakeholders, including **EDRi**, **civil society**, **media** and **journalists** organisations, **doctors** and **lawyers** associations, **internet companies**, **trade associations**, the **European Data Protection Supervisor** (EDPS), the **European Data Protection Board** (EDPB), **academics** and **think tanks**.

Yet, after two years of inter-institutional negotiations, the Council and the Parliament have **failed** to build a framework that provides **sufficient safeguards** and remains bulletproof against abuses. The following non-exhaustive analysis is based on the final **text approved by the Council's Permanent Representatives** on 25 January 2023.

A quick look back

After the Commission released its legislative proposals in April 2018, the Council quickly agreed on its position (also named "general approach" in EU jargon) in December of the same year. It left however, **eight Member States** greatly concerned by **the lack of consideration for "checks and balances"** and "guarantees for the protection of fundamental rights". These concerns **were shared** by EDRi which evaluated the Council's text as a severe deterioration of the few provisions that were meant to safeguard fundamental rights in the Commission's original text.

For its part, the European Parliament adopted its report at the end of 2020 containing important improvements stemming from the Rapporteur's original draft to better protect people and the rule of law against law enforcement overreach. Unfortunately, **major compromises** were also made in order to reach a majority, which **led us to fear** for the fate of the new provisions protecting fundamental rights during the trilogue negotiations.

Meanwhile, the Commission obtained from the Council the mandate to start bilateral negotiations with the United States (US) on **cross-border access to data** and represent the EU at the Council of Europe's negotiations to adopt a **Second Additional Protocol to the Budapest Convention on Cybercrime**. We saw this as a **worrying disregard** for the EU's democratic legislative process as it ignored the position of the co-legislator, the European Parliament.

Thankfully, the Commission quickly **stopped** the negotiations with the US after realising its own negotiation position was unclear and unstable without a common European approach. With the adoption of the e-Evidence proposals, they are expected to resume at once.

The crux of the debate: what's left of the notification system?

As advocated for by **EDRi** and **others**, a **key solution** to fixing the worst flaws in the original e-Evidence proposal was to set up a **notification mechanism**: this mechanism would require the issuing authority seeking to access data to send its order to at least a second Member State's judicial authority before being executed by the addressee (i.e. the service provider). The second authority would have the responsibility to verify the legality and proportionality of foreign data access orders – rejecting those that violate fundamental rights, similar to its responsibility under existing mutual legal assistance agreements

EDRi recommended to give this duty to (1) the judicial authorities where the person whose personal data is requested resides (the 'affected State') as they are best placed to know about their potential special protected status limiting access (a journalist, a lawyer, a social worker or a medical professional); (2) the judicial authorities in the 'executing State', where the company is officially located or established in order to guarantee legal certainty.

While the Parliament included a **fairly robust notification regime** in its position, the **Council's version** was far from being comprehensive and protective in practice, notably in light of the very minimalistic list of refusal grounds.

As a result of the trilogue negotiations, the notification regime has been **reduced to a trickle** and is basically toothless:

- No notification is required for **preservation orders**;
- No notification is required for **production orders** that seek subscriber information and traffic data "requested for the sole purpose of identifying the user" – the notification only happens when traffic and content data is requested. **Consequences can be severe** when these orders target the identity of journalists' sources or whistle-blowers or doctors' and social workers' patients;
- The issuing Member State is exempted from notifying its counterpart when it has "reasonable grounds to believe that the offence is committed in the issuing State, and where the person whose data are sought resides in the issuing State." This "**residency criteria**" is extremely problematic because (1) this assessment is left entirely to the discretion of the issuing State's investigative authority, which has considerable **interests in avoiding the notification procedure** perceived as 'too cumbersome' and the risk to have their order refused by the executing State, and (2) the factors that should guide the issuing State to make that assessment are excessively vague and can be easily twisted (the person has "family ties or economic connections" or "manifested the intention to settle in that Member State" or "established the habitual centre of his or her interests in a particular Member State or has the intention to do"). This represents a **major crack** in the notification system;
- None of the legislators' position included the **affected State** as part of the notification mechanism; therefore the notification is only sent to the executing State authorities. This is detrimental in cases where neither the issuing nor the executing authorities are aware of immunities **protecting a person** under a third State's national law;
- The **active validation** of a foreign order by the executing State is not required. As soon as the **deadline** passes (10 days as a general rule, 8 hours in emergency cases), the service provider must transfer the requested data even if the executing authority did not give its green light;
- When the issuing authority deems the **case urgent**, the notification has no suspensive effect, which means that the service provider must transfer the data as soon as possible and regardless whether or not the executing State had the time to verify the order.

Consequently, the application of the notification mechanism will likely be the **exception rather than the rule** in the daily practice of law enforcement and judicial authorities.

Lastly, the co-legislators seem to have struggled to find a compromise on the **responsibility of the executing State** at the stage of orders verification. Article 10a indicates an obligation to assess the order: "the enforcing authority shall (…) assess the information set out in the Order and, where appropriate, raise one or more of the following grounds for refusing the Order". However, recital 42b says "it should have the right to assess" and raise refusal grounds "based on a mandatory and due analysis of the information". This troubling contradiction shows a **fragile agreement** between the Parliament and the Council and raises a lot of **legal uncertainty**.

The distinction is however of great importance. Member States, and especially Ireland where most prevailing service providers are located, have criticised the notification mechanism as excessively **burdensome** for the executing State. Without a **clear obligation** to validate foreign orders, the executing authority could not even review them and dispose of its responsibility.

This text surely fails to meet the **quality of law requirement** established by the European Court of Human Rights, demanding surveillance laws to be sufficiently clear and foreseeable. In practice, it will mostly impact service providers and the rights of affected individuals – at least until the Court of Justice of the European Union (CJEU) gets the opportunity to clarify this provision.

Politically-motivated abuses and rule of law concerns

The risk that this **law enforcement instrument is abused** to target journalists, human rights defenders, activists, political opponents and lawyers is substantial. The final text attempts to address these concerns but fails to outweigh the multiple shortcomings the law suffers from.

For example, the executing State, when notified or at the enforcement stage (i.e. in the rare cases where the service provider has not executed the order and the authorities in the executing State have to intervene to force compliance), can block an order if there is a risk of a fundamental right breach. However, the text is excessively convoluted, restricting that power to "exceptional situations" and "manifest" breaches, requiring "substantial grounds to believe, on the basis of specific and objective evidence" and "in the particular circumstances of the case" (Articles 10a(1)(b) and 14(4)(g)).

It renders the protection of fundamental rights almost meaningless. The notion of such situations being exceptional is also at **odds with the findings of the PEGA Committee** on **systemic abuse of state surveillance powers**.

Regarding immunities and privileges, it is positive that they feature in the list of grounds for refusal. Nevertheless, and given the many loopholes of the notification system mentioned above, the likelihood that this provision will be used by the executing State is low. It is also doubtful that the issuing State will use the possibility under Article 5(7) to "seek clarification" in case it believes that the data sought is protected by immunities and privileges under the law of the executing State. In the majority of cases, the service providers will remain the sole defence against law enforcement overreach. Unfortunately, **their power to halt the execution of orders is limited and clearly disincentivised**: they can only raise concerns "based solely on the information contained in the" order.

The way to handle orders issued by Member States with systemic rule of law deficiencies (subjected to Article 7(1) of Treaty of the European Union) was also a sticky point during the negotiations. The power to refuse their orders did not pass the test of the trilogues. Only a timid reference was added in Recital 42d). It is watered down by the call on the executing State to take the specificities of the case into account, notably "the concerned person's personal situation, "the nature of the offence" and "the factual context" before determining that the right to a fair trial could be breached.

The weak protections against fundamental rights violations will notably impact people residing in Member States with **systemic rule of law problems**. Because of e-Evidence, they do not get better protection of their fundamental rights by using a service provider in another country – unlike for example activists in Russia who can feel reassured that Google or Microsoft will not provide their data to the Russian government without scrutiny.

Other notable issues

Other problematic aspects of the final compromise that are worth pointing out include:

- The issue of discriminatory prejudice is only acknowledged in a recital (10(b)) but the operative safeguards are clearly lacking, as demonstrated above.
- It is justified that IP addresses deserve a lesser level of protection when sought for the purpose of identifying a suspect. **This stands at odds with the CJEU case law** (at least for now).
- Article 5(6)(c) on protection of professional privileges only covers situations where cloud infrastructure is provided to professionals protected by that professional privilege, **which excludes e.g. independent journalists using email services offered to the general public for their work**.
- Previous draft provisions regulating the re-use, transfer and admissibility of data obtained via an e-Evidence order have been deleted. **Only the rules of Law Enforcement Directive apply (Article 9(3) and recital 36), which are rather limited** in what conditions can be imposed for transfer between Member States.
- The issuing State is granted the leeway to withhold for a possibly long and indeterminate period of time the information to the individual that their data has been accessed. However, the fundamental rights to access effective remedies and to a fair trial require that the suspected person is informed as soon as possible in the process. **There is a concern that "gag orders" are excessively used as a matter of course, rather than exceptionally when strictly required**.
- The right to an effective remedy can only be exercised before a court in the issuing State in accordance with its national law, which can represent **a considerable barrier for individuals to exercise their rights** (travel, language, etc.). It is unclear how "the guarantees of fundamental rights in the enforcing State" will be taken account in the course of the court proceedings.

Next steps

Following the validation of EU member states' ambassadors of the compromise text, the responsible Committee of the European Parliament, the LIBE Committee (Civil Liberties, Justice and Home Affairs), also adopted it with a large majority on 31 January.

In the coming months, the Justice and Home Affairs Council composed of Ministers is expected to give its approval, while **the text will pass a final vote in the Parliament's plenary**. In view of the many shortcomings highlighted above, EDRi and its partners will call on Members of the European Parliament to stand up for fundamental rights by rejecting the e-Evidence proposals.

Chloé Berthélémy

Senior Policy Advisor

Twitter: **@ChloeBerny**