EDRi

EUROPEAN DIGITAL RIGHTS

Demonstrating gaps in the e-Evidence Regulation

Examples of fundamental rights infringements related to cross-border access to data in criminal matters

This publication has been co-authored by the following organisations:

EDRi

EUROPEAN MAGAZINE MEDIA ASSOCIATION

hope
European Hospital and Healthcare Federation

FREE KNOWLEDGE ADVOCACY GROUP EU

CPJ
COMMITTEE TO PROTECT JOURNALISTS

WIKIMEDIA FRANCE

EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

ENPA
EUROPEAN NEWSPAPER PUBLISHERS' ASSOCIATION

IT-Political Association of Denmark

EBU
OPERATING EUROVISION AND EURORADIO

VDZ
Verband Deutscher Zeitschriftenverleger

DeutscherAnwaltVerein

Fair Trials

CPME
COMITÉ PERMANENT DES MÉDECINS EUROPÉENS
STANDING COMMITTEE OF EUROPEAN DOCTORS

Index

Introduction

This compendium of scenarios aims at contributing to the current debate at European level on the adoption of a new Regulation on European Production and Preservation Orders in criminal matters ("e-Evidence Regulation"). The organisations, representing a diverse group of stakeholders that co-authored this document, urge the European Parliament and the Council to uphold a high level of fundamental rights safeguards during their negotiations.

Following a joint letter sent on 18 May 2021 highlighting our concerns,[1] this compendium complements our recommendations by showcasing four different scenarios in which the e-Evidence Regulation would lead to serious fundamental rights harms. This type of analysis was already carried out by the German Ministry of Justice in May 2019 in a background paper.[2]

The scenarios mentioned in our compendium demonstrate the disproportionate impact of the future Regulation (1) on the work of journalists, (2) the protection of sensitive health data, (3) the freedom to protest in Member States with systemic rule of law issues, and (4) the right to a fair trial - if some of its proposals remain in the final text.

The scenarios prepared are structured in a way that highlights the fundamental rights at stake, describes hypothetical problematic situations involving the cross-border access to personal data and explains the necessary safeguards advocated for to mitigate these fundamental rights harms. The Commission's original proposals have been taken as a basis to come up with these scenarios, except where otherwise indicated: in the latter cases, we address the Council's and the Parliament's positions and the issues currently discussed in the trialogue negotiations.

The authoring organisations look forward to discussing with EU lawmakers in the next steps of the negotiations and remain at their disposal for further information.

---

[1] **EDRi and al., Trilogue negotiations on the e-Evidence proposal. European media and journalists, civil society groups, professional organisations and technology companies call on decision makers to protect fundamental rights, 18 May 2021,** https://edri.org/wp-content/uploads/2021/05/20210518_EevidenceJointLetter_18May2021.pdf

[2] **German Ministry of Justice, Background Paper, 31 Mai 2019, obtained by NetzPolitik:** https://cdn.netzpolitik.org/wp-upload/2019/07/Hintergrundpapier-e-Evidence-cl.pdf.pdf

Recommendations

In light of the scenarios below, the undersigned organisations would like to make the following recommendations to EU policymakers:

- Introduce a mandatory and automatic notification procedure for the executing State with suspensive effect, including (1) a duty to ensure all relevant immunities and privileges are properly considered and in case of violating orders, (2) an obligation to invoke grounds for refusal based on the EU Charter of Fundamental Rights;
- Give a clear definition of immunities and privileges which encompasses rules related to media freedom, freedom of information, professional secrecy and medical confidentiality;
- Involve the affected State in order to properly take into account the immunities and privileges when relevant;
- Provide clear information immediately to the person whose data is sought, unless otherwise authorised by a court or an independent administrative authority;
- Ensure access to effective remedies both in the issuing and executing States;
- Give early access of the case-file to the defence and enable the use of e-Evidence orders on behalf of a suspected or accused person;
- Provide the same level of protection for all types of data;
- Ensure that every order contains a summary of the underlying facts and a description of the offence;
- Give service providers the possibility to halt an order if orders are "manifestly abusive", i.e. they are not restricted to a limited set of data, timeframe or the number of persons.

01 Protecting media freedom and sources

Scenario

Emy is a journalist who lives in Member State X. She is investigating a serious case of fraud in Member State Y. This fraud case is subject to a custodial sentence of at least three years in Member State Y, but not where Emy lives.

Emy is in touch with Clara, who lives in Member State Y. Clara has incriminating information about the fraud case which she sends to Emy by email.

Member State Y then opens a criminal investigation against Clara because they suspect her involvement in the fraud.

Even though Clara has deleted her email exchanges with Emy, investigators analysing her computer can see that they have been in touch and want to know the content of the emails. Emy's email provider is based in her country - Member State X. The authorities in Clara's country, Member State Y, therefore issue a European Production Order asking Emy's email provider to provide them with the data of Emy & Clara's email exchanges.

How this scenario would be handled by the proposed e-Evidence proposal:

According to the European Commission's original e-Evidence proposal, upon notification of the European Production Order from the competent authority in Member State Y, the email provider must execute the Order and provide the requesting authority in Member State Y with the data held by Emy - unless it can determine that it manifestly violates the Charter of fundamental rights or is manifestly abusive.

The transmission of the requested data is issued without the competent authorities in Member State X being notified of the cross-border exchange of information, and irrespective of the fact that the crime is not recognised in the same way in both Member States. Member State Y may not know that Emy is a journalist residing in Member State X. Furthermore, the execution of this order could lead to the disclosure of other associated information, including identities of additional informants, and trigger subsequent proceedings.

Two negative outcomes of the current e-Evidence proposal for media freedom and the protection of sources:

1. Emy is affected by a pending criminal investigation in a different Member State. As a resident of Member State X, she is protected by her national laws including rules related to press and media freedom. The e-Evidence Proposal jeopardises this principle by not involving the authorities in her Member State of residence and might put her journalistic work, journalistic sources, the editorial secrecy and general media and press freedom at risk.

2. The e-Evidence proposal could hinder freedom of information as informants' willingness to collaborate with journalists might decrease, possibly reducing the information available for public democratic scrutiny.

Necessary safeguards

The e-Evidence Proposal should be changed to include the following five safeguards:

1. Mandatory and automatic notification procedures for the executing State with suspensive effect

Any order should be addressed simultaneously with the service provider and with the competent authority in the executing Member State where the service provider is established. This way, the competent authority in Member State X would be able to oppose the execution of the Order on the basis that the content, qualifying as journalistic content, is protected under national law.

In addition, data should only be transferred when the competent authority in the executing Member State has validated the Order. If the executing authority fails to provide its assessment within 10 days, the service provider should not assume a green light. In this case, clarification should be sought.

2. Immediately inform the data subject unless otherwise authorised by a court or an independent administrative authority & ensure access to effective remedies

A requirement to inform the data owner as soon as possible would ensure that Emy is aware that her conversations were disclosed and can challenge the Order before a court in one of the Member States involved in order to seek redress.

3. Involve the affected State in order to properly take into account the immunities and privileges when relevant

In cases where Emy does not reside in the executing nor the issuing State, immunities and privileges in that third country should be checked.

4. Provide the same level of protection for all types of data

All types of data should have the same level of protection. For example, lowering the protection for identification data (categorised as "subscriber data" and "data for the sole purpose of identifying the user, the IP addresses and, where necessary, the relevant source ports and time stamp (date/time), or technical equivalents of these identifiers" under the most recent agreements of the trilogues) could lead to scenarios where the identity of an informant is revealed and consequently journalistic sources are disclosed and fundamental rights endangered.

5. Give clear definition of immunities and privileges which encompasses rules related to media freedom and freedom of information

The whole media sector and all journalistic activities should be protected and covered by immunities and privileges.

Fundamental rights at stake

Media and press freedom | Editorial secrecy | Freedom of information | Protection of journalists | Including protection of sources

For further information, please contact:
Ilias Konteas, Executive Director, European Magazine Media Association (EMMA) – European Newspaper Publishers' Association (ENPA)
Ilias.Konteas@magazinemedia.eu; Ilias.Konteas@enpa.eu
Wouter Gekiere, Head of Brussels Office, European Broadcasting Union (EBU)
gekiere@ebu.ch

02

Protecting medical confidentiality and health data

Scenario

A physician, Anna, buys a summer house in Member State X and decides to transform it for local tourism purposes. Anna applies for regional development funding to support the house renovation. The funds are granted and the renovation work is pursued. Anna invites several public figures to spend their holidays in the house for free. This attracts the attention of the authorities in Member State X. They suspect that Anna is involved in money laundering operations and misappropriation of public funds. A prosecutor in Member State X issues a European Production Order under the e-Evidence Regulation addressed to Anna's cloud storage service provider, as they have reason to believe that the cloud account contains evidence for the case. The authority therefore requests all content data including emails, text files, documents, images and videos, stored on their servers on behalf of Anna.

Anna has registered two accounts under her name, one for professional purposes and one for personal administrative matters. The professional cloud storage account contains several patient files, including sensitive health data in the format of images (scans), documents, audio files and even videos. Unaware of the confidential nature of the data stored by this customer, the cloud service provider executes the order and provides the requested data of both accounts. The judicial authorities in Member State Y where the cloud service provider is legally established are not aware that the order was received and executed, nor do the judicial authorities in Member State Z where Anna has her main residence and is established.

Necessary safeguards

1. Prevent repurposing and "fishing expeditions"

In the Commission's proposal, the information contained in the Production Orders is very limited and does not enable the recipient to evaluate if orders effectively comply with the principles of necessity and proportionality.

The future Regulation should require that the order contains a summary of the underlying facts and a description of the offence. There should be a possibility for service providers to halt an order if it is "manifestly abusive" and if it is not restricted to a limited set of data, timeframe or the number of persons.

There is no safeguard to prevent the unlawful repurposing of the data obtained (in line with the purpose limitation principle) or "fishing" expeditions, whereby law enforcement authorities could request untargeted, massive amounts of data without justifications in order to uncover incriminating evidence. In practice, authorities sometimes send very broad requests which can be unlimited as to the time period, without specifying what data is relevant and why it is important for the investigation.

In the present case, the issuing authority should specify which account it wants to access data from, narrowing down its request to data where there is reasonable suspicion/probable cause that it will help the investigation (probably not videos, images, etc.), as well as to a specific timeframe.

2. Ensure oversight and respect professional secrecy

Access to medical data, subject to professional secrecy, should be limited to strictly defined cases, where it is absolutely necessary for the criminal proceedings. Health data deserves the same level of protection online as offline.[3] Private service providers do not have the resources, and even less the legal competence, to identify and select only data necessary and proportionate for a specific criminal case. They also do not possess the adequate knowledge to assess the legality of an order.

In the Commission's proposal, the issuing authorities are expected to consider immunities and privileges pursuant to the national law of the Member State where the service provider is established, in particular when this provides a higher level of protection than its domestic law. This safeguard is unlikely to offer sufficient protection in practice, for example due to the lack of detailed knowledge of national laws granting immunities and privileges in all 27 Member States.

The "e-Evidence" Regulation should therefore also include a notification mechanism, with suspensive effect, requiring the validation of orders by independent judicial authorities in the executing Member State, and in the affected Member State where applicable.

This review mechanism ensures that orders are complete and legitimate, proportionate and necessary and can be rejected if incompatible with the EU Charter of Fundamental Rights. In the example above, the issuing authorities of Member State X would reasonably determine that Anna is licensed in Member State Z and therefore should send a copy of their order to the competent authorities there, in addition to Member State Y (where the cloud service provider is legally established).

3. Specificities for telemedicines and health data as e-Evidence

Telemedicine services and service providers offering secure networks for the exchange of patient information between health professionals, patients, national health systems and/or health insurance funds, for which the storage of health data is not the defining component of the service provided to the user, **should be excluded from the scope of the regulation (Recital 16, Commission's proposal).**

For other cases (for example the storage of electronic health records) and **when health data are requested to serve as evidence** (for example in cases of crimes related to dissemination of infectious diseases, frauds involving forged health bills, analysis examinations results, incorrect health results, etc.), **service providers should only be allowed to disclose confidential medical information if a prior review and approval has been given by a competent authority, national medical association (NMA) or medical regulator.** This requirement is needed where the medical professional, a private hospital, a clinic or a laboratory are the direct recipients of the order (because they provide health data storage services). Competent authorities, NMAs or medical regulators have the responsibility to verify and waive medical confidentiality and professional secrecy, guaranteeing that health data are correctly interpreted, adequately used and limited to what is necessary.

Lastly, where a service provider stores health data on behalf of a clinic or any other medical company (Article 5(6), Commission's proposal), orders should only be addressed to the service provider if a court or an independent administrative authority confirms that it might jeopardise the investigation. The service provider should also be allowed to inform their client, unless otherwise indicated by the court or the independent administrative authority.

Without these additional safeguards, **the e-Evidence Regulation risks violating professional secrecy and medical confidentiality legal obligations that doctors have to comply with as well as patients' rights to privacy and to dignity.**

Fundamental rights at stake

Right to privacy

Right to personal data protection

Right to human dignity

Legal obligation and ethical duty of medical confidentiality and professional secrecy

For further information, please contact:
Sara Roda, Senior Policy Advisor, Standing Committee of European Doctors
sara.roda@cpme.eu

---

3 **See CPME response to the public on consultation on a set of European digital principles, July 2021.** https://www.cpme.eu/cpme-response-to-public-on-consultation-on-digital-principles

03 Protecting our right to protest and the rule of law in the EU

Scenario

In 2015, massive, nationwide protests took place in Member State X, contesting several decisions of the government and calling for stronger democratic accountability. Protesters mostly used Facebook to organise and coordinate the protests. A parliamentary commission subsequently confirmed that protesters had been illegally monitored and wiretapped. More than 2 500 people became victims of a surveillance operation, involving the creation of personal profiles based on social media information (e.g. Facebook posts, events), the interception of electronic communications and photography of protesters. Some targeted participants were summoned to the police station and threatened to stop their protest activities by using the collected data against them.

If the proposed e-Evidence Regulation is adopted based on the Commission's and Council's versions, the following hypothetical example shows how this data collection instrument could have further impacted the fundamental and civil rights of protesters.

From the information collected on social media, the police noticed that protestors were using Wikipedia, the online encyclopedia edited by volunteers, to report and document the story of the movement, police violence and the government's actions in response to the protests and occupations. As the police intend to find the leaders of the movement, they seek to identify the authors of several Wikipedia articles (i.e. the editing log of the Wikipedia pages). They issue a European Production Order to access identifying data held by Wikimedia, notably the IP

addresses linked to the editing of the articles that are normally retained for content moderation purposes.

Legal requests related to Wikipedia articles and websites are handled by the Wikimedia Foundation which is obliged by the Regulation to appoint a legal representative in the EU. Therefore, Wikimedia's EU legal representative receives the order. While Wikimedia is concerned that the order violates the Charter of Fundamental Rights, they decide to comply with the order to avoid the risk of sanctions. The competent authorities in the Member State of establishment Y are not aware that the order was received and executed, as this is not foreseen in the procedure.

After receiving the IP addresses of the authors, the police rapidly use domestic investigative measures to link them to civil identities, allowing the police to target the persons with intrusive and intimidating measures to further suppress dissent.

Necessary safeguards

1. Prevent misuse in Member States where rule of law is weakened

Illegal investigation scandals are recurrent in Member State X. Recently, its domestic national security agencies were accused of eavesdropping on more than 25 opposition politicians in the run-up to the general election as well as dozens of other people who took part in civil society protests against the government.

These scandals represent systemic rule of law problems which have received international criticism on numerous occasions, including in a resolution from the European Parliament. However, the fundamental rights safeguards in the EU Treaties have proven ineffective in addressing the situation, in part because Member State X is not the only Member State with serious rule of law problems, and initiating procedures under the Treaty of the European Union Article 7 requires unanimity among the other Member States.

Introducing the e-Evidence instrument in Member States where the independence of the judiciary is not guaranteed would be incredibly risky for the protection of fundamental rights. To alleviate the inherent risks of abuse, we recommend to introduce **a regime of systematic**

involvement of the authorities of the executing Member State, as early as possible in the process, for all kinds of orders and data categories sought, with the obligation to review compliance of orders with the Charter and to raise grounds for refusal on that basis. In the example above, the judicial authorities in the Member State where the legal representative of Wikimedia was appointed should be responsible to review the Production Order and refuse it.

Furthermore, if the issuing authority decides to keep the order confidential from the persons whose data is sought, it should be required to justify why. This would ensure that European Production Orders are used solely in the context of criminal proceedings and for prosecution purposes, and not instrumentalised as part of secret state surveillance practices. In our example, notifying the affected individuals would prevent the use of the e-Evidence Regulation to hamper future protests which could lead to significant chilling effects on civil society and reinforce the backsliding of the rule of law.

2. Prevent unlawful transfers of data and unjustified identity disclosure

Under the Commission's proposal and the Council's version, Wikipedia IP addresses would be considered "access data". This categorisation means that its Production Order requires no validation from a judge, no notification to executing authorities and is available for all types of criminal offences, even petty crimes. Under the most recent agreements of the trilogues, it would be considered traffic data but a special regime applies "for the sole purpose of identifying the user, the IP addresses and, where necessary, the relevant source ports and time stamp (date/time), or technical equivalents of these identifiers".

The creation of a "special regime" which effectively treats certain processing of traffic data as access to subscriber data is worrying, as it maintains the "access data" carve-out. **It is essential for the future Regulation to be in line with the most recent Court of Justice of the European Union case law (notably C-746/18 – Prokuratuur) that holds that even access to a small subset of traffic data may provide precise information about a person's private life and therefore requires more protections.**

It should be mandatory for the executing authority to give its explicit approval before any Production Order can be executed (suspensive effects). This would avoid situations where it is too late for the executing authority to object to an order as the service provider already gave out

the data. This guarantees that all fundamental rights are respected before getting access to the person's identity. Once the police learn the protesters' identity, they will not forget or delete it just because the transfer of identifying data has been declared unlawful.

Fundamental rights at stake

Freedom of protest

Freedom of expression

Right to privacy

Freedom to receive and impart information

For further information, please contact:
Chloé Berthélémy, Policy Advisor, European Digital Rights
chloe.berthelemy@edri.org
Dimitar Dimitrov, EU Policy Director, Free Knowledge Advocacy Group EU (Wikimedia Brussels)
dimi@wikimedia.be

04 Protecting our right to a fair trial

Scenario

An authority in Member State X is investigating a case of the online dissemination of child sexual abuse material (an offence covered by the e-Evidence Regulation under Article 5(4)) on a small online forum. They request subscriber and traffic data associated with the disseminating account that could help identify the user with a European Production Order. The Order specifies that the foreign service provider running the website must refrain from informing the suspected users in order to not obstruct the ongoing criminal investigation. The police receives 3 relevant IP addresses and retrieves the corresponding subscriber data (name and address) of the users to which the IP addresses were assigned at the time of the upload.

Nicholas is identified as one of the potential suspects. His house is searched and all his connected devices (computer and phones) are seized for examination.

Months later, Nicholas and his lawyer obtain access to the prosecution casefiles, discover the exact time of the upload, and realise that at the time Nicholas was on holiday, hitchhiking through Europe. Nicholas remembers that he was connected to the WiFi of a café where he had stopped for a couple of hours on the day and time of the offence. When logging in, the café's webpage had informed him that the MAC address[4] of his computer would be retained in log files for security purposes. His lawyer therefore seeks to request the data from the café. This data would help prove his innocence since he was not physically

in the country indicated by the incriminating IP address. Unfortunately, the procedure to access the data is long and difficult due to the lack of appropriate instruments, the language barrier and the fact that the order addressee is located abroad. By the time their request is accepted, the café informs them that they have already deleted the data related to that period.[5]

Fortunately, it is later discovered that there an error was made in the data production request procedure. The investigative authority had failed to convert the time of the upload to the correct time zone. As a consequence and because the IP addresses are dynamic, the results were incorrect by three hours - thus wrongly attributing the offence to Nicholas' internet connection at home.

---

[4] A media access control address (MAC address) is a unique identifier assigned to the network interface card, present in every connected device, for use as a hardware address in communications with a certain network.

[5] In the present case the data was already deleted but it is also important to stress that some service providers may also refuse data subject access requests for information held in systems log files, which could still be disclosed as "access data" in a Production Order, based on (perceived) exemptions from GDPR Article 15. A decision from the Danish DPA (2005-632-0077) excluded personal data in system log files from the scope of a subject access request if the information was processed solely for systems-oriented purposes, e.g. information security, not directly related to the data subject.

Necessary safeguards

1. Notifying the affected person by default

Timing is an important factor in criminal proceedings for both the defence and the prosecution. It is advantageous for the investigative authorities to keep the suspects in the dark, unaware that they are being subjected to certain surveillance measures or a criminal investigation, in order to facilitate the collection of incriminating evidence.

However, the fundamental right to access effective remedies and the right to a fair trial require that the suspected person is informed as early 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. Notifying the suspect ensures that the defence has enough time to eventually challenge the legality of the order and build their case by gathering exculpatory evidence.

As a result **we recommend modifying Article 17 (Commission's proposal) to make the notification to the affected person mandatory as soon as possible after the interference occurs. The information about the order should be provided without undue delay and restriction even in the absence of ensuing criminal proceedings and unless otherwise decided by a court or an independent administrative authority.** Concerns about the destruction of evidence should the person be informed of the investigation may be alleviated by the availability and use of preservation orders.

Access to this information is all the more important since being prosecuted and convicted of such serious crimes can have severe implications for the accused. Even if the person is eventually acquitted or has charges dropped, it can result in long-term stigma, loss of employment prospects, destruction of family relationships, and civil liberties in addition to the potential for loss of liberty and the imposition of severe penalties. Specific measures in the e-Evidence Regulation should be introduced to guarantee the right to the presumption of innocence during an investigation.

2. Provide the defence with early access to the casefile and evidence-gathering tools

The (1) lack of early access to the casefile and (2) to evidence-gathering tools for the defence weakens the right to a fair trial and the principle of equality of arms. **Yet, the principle of equality of arms is an essential guarantee of an accused's right to defend themselves.** It ensures that the accused has a genuine opportunity to prepare and present their case, and to contest the arguments and evidence put before the court, on a footing equal to that of the prosecution.

1. Access by the defence to the casefile and its participation in the review of evidence gathered represent an additional safeguard against human mistakes (e.g. failure to convert to the correct time zone like in our example) and miscarriages of justice.

2. In practice, it is extremely difficult, if not impossible, for the defence to use the cross-border evidence gathering mechanisms to gather evidence abroad.[6] It can only trust the objectivity of law enforcement authorities to gather both incriminatory and exculpatory information.

Therefore, the future Regulation should (1) give early access to the casefile and (2) empower the defence to request a production or preservation order on behalf of a suspected or accused person in order to gather evidence on equal terms with the prosecution. Member States or service providers receiving such requests should have the obligation to process them with the same urgency as requests received from law enforcement authorities.

Fundamental rights at stake

Right to a fair trial

Right to access effective remedies

For further information, please contact:
Martin Sacleux, Legal Advisor, Council of Bars and Law Societies of Europe (CCBE)
sacleux@ccbe.eu
Laure Baudrihaye-Gérard, Legal Director (Europe), FairTrials
laure.baudrihaye@fairtrials.net

---

6 **FairTrials, Policy Brief: The impact on the procedural rights of defendants of cross-border access to electronic data through judicial cooperation in criminal matters, October 2018, available at:** https://www.fairtrials.org/sites/default/files/JUD-IT-Fair-Trials-Policy-Brief-October-2018.pdf

Press enquiries
press@edri.org

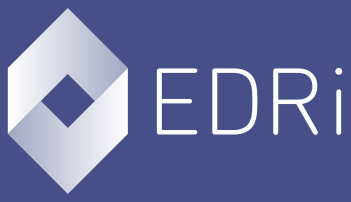
Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us
Rue Belliard 12
1040 Brussels
Belgium

Follow us
Twitter
Facebook
LinkedIn
Youtube

The EDRi Brussels office lead and main contributor for this piece of work was Chloé Berthélémy, Policy Advisor. We would like to thank all organisations involved and give a special nod to Gail Rego for her review.



EUROPEAN DIGITAL RIGHTS

European Digital Rights (EDRi) is the biggest European network defending rights and freedoms online. We promote, protect and uphold human rights and the rule of law in the digital environment, including the right to privacy, data protection, freedom of expression and information.

www.edri.org