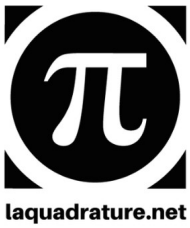

Joint civil society response to the Commission's call for evidence for an impact assessment on retention of data by service providers for criminal proceedings

Table of Contents

This submission was submitted on 18 June 2025 and gathers the input of the following civil society organisations:

European Digital Rights (EDRi) is a network of 50+ NGOs across Europe and beyond that defend and promote human rights in the digital era.

IT-Pol Denmark (member of EDRi) works to promote privacy and freedom in the information society and focuses on the interplay of technology, law and politics.

Privacy International (member of EDRi) researches and advocates globally against government and corporate abuses of data and technology.

Chaos Computer Club (member of EDRi) is the largest hacker organisation in Europe and has been mediating between the conflicting priorities of technical and social developments for over forty years.

Epicenter.works – for digital rights (member of EDRi), formerly "Working group data retention Austria", plaintiff in the CJEU case annulling the EU Data Retention Directive in 2014.

Digitalcourage (member of EDRi) has been working for a livable world in the digital age since 1987, advocating for fundamental rights, privacy, and the protection of personal data.

Electronic Privacy Information Center (EPIC) (member of EDRi) is a public interest research center founded to protect privacy, freedom of expression, and democratic values in the information age.

Electronic Frontier Foundation (member of EDRi) champions user privacy, free expression, and innovation through litigation, policy analysis, grassroot activism, and technology development.

Digitale Gesellschaft (member of EDRi) promotes digital rights and works for an open digital society since 2010.

La Quadrature du Net (member of EDRi) promotes and defends fundamental freedoms in the digital world. It fights against censorship and surveillance, and works for a free, decentralised and empowering Internet.

Executive Summary

We thank the European Commission for the opportunity to express our shared concerns with regards to the introduction of new rules at EU level on the retention of data by service providers for law enforcement purposes.

We strongly oppose the adoption of a new EU legal instrument forcing electronic communications service providers to massively retain their users' traffic and location data beyond what is necessary for the provision of the service and billing purposes (as per the ePrivacy Directive 2002/58/EC). We hold that such obligation:

- constitutes mass surveillance, which unacceptably undermines the rights to privacy and data protection and thus, endangers the exercise of other fundamental rights enabled by them such as freedom of expression and information, freedom of assembly and association, the right to a fair trial, to health care, to social protection and social assistance, etc.;
- has been found contrary to the EU Charter of Fundamental Rights by the Court of Justice of the European Union (CJEU);
- creates inadmissible data security risks, considering that the vast amounts of personal data retained for law enforcement are vulnerable to cyberattacks (which happen on a regular basis with disastrous consequences for people affected).[1]

It is our recommendation that the Commission prioritises the launching of infringement procedures against Member States whose data retention legal framework does not comply with the CJEU case law. Based on the most recent reports and surveys[2], it would concern a majority of Member States. Once all infringing national laws have been brought in line with EU law as interpreted by the Court of Justice, the Commission could carry out a proper assessment of impacts, including on the respect for fundamental rights, and eventually consider an EU instrument to remedy shortcomings.

We would also like to stress that there is still no scientifically proven link between indiscriminate data retention and impact on crime or crime clearance. **Considering the European Commission's strong commitment to evidence-based policy-making and the Charter requirement of necessity[3] for any interference with fundamental rights, the general and indiscriminate retention of traffic and location data as a policy option must be rejected**.

This submission is based on the Commission's call for evidence for an impact assessment (Ares(2025)4081079) and the documents produced by the High Level Group on "Access to Data for Effective Law Enforcement".[4]

---

1 EDPB, Hellenic DPA: Fines imposed to telecommunications companies due to personal data breach and illegal data processing, 3 February 2022, https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-imposed-telecommunications-companies-due-personal-data_en
Anton Mous, Data of 70,000 customers of Belgian virtual telecom operators leaked, *Cybernews*, 16 May 2025, https://cybernews.com/security/data-belgian-virtual-telecom-operators-leaked/
FBI, Joint Statement from FBI and CISA on the People's Republic of China Targeting of Commercial Telecommunications Infrastructure, 13 November 2024, https://www.fbi.gov/news/press-releases/joint-statement-from-fbi-and-cisa-on-the-peoples-republic-of-china-targeting-of-commercial-telecommunications-infrastructure
Jonathan Greig, Largest telecom in Africa warns of cyber incident exposing customer data, *The Record*, 25 April 2025, https://therecord.media/largest-african-telecom-warns-of-data-exposure

2 *The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU*, Eurojust and EJCN, November 2024 https://www.eurojust.europa.eu/publication/effect-court-justice-european-union-case-law-national-data-retention-regimes-judicial-cooperation
Fundamental Rights Agency (FRA), Fundamental Rights Report 2023, pp. 185-187 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2023-fundamental-rights-report-2023_en_1.pdf
Council, Data retention - Situation in Member States, Working Paper 3103/2019 INIT, 06 March 2019, https://cdn.netzpolitik.org/wp-upload/2019/06/VDS-EU-Stand-Umsetzung.WK-3103-2019-INIT.pdf

3 Article 52(1) of the Charter of Fundamental Rights

4 https://home-affairs.ec.europa.eu/networks/high-level-group-hlg-access-data-effective-law-enforcement_en

We call on the Commission to consider the six following issues for its current impact assessment process, which reflect the structure of our written submission:

- Member States' current data retention practices are a rule of law crisis
- Data retention and access to retained data are separate interferences
- There is no reliable evidence that mandatory data retention is necessary
- Data retention for OTT (number-independent) providers threatens the right to anonymity online
- Assessment of the CJEU case law for retention of IP addresses (HADOPI judgment): technical solutions cannot prevent serious interference with the right to privacy in all circumstances
- Data retention of source IP addresses and port numbers may lead to potentially serious interference with the right to privacy

1. Member States' current data retention practices are a rule of law crisis

After the annulment of the Data Retention Directive 2006/24 by the Court of Justice (CJEU) in April 2014, Member States did not repeal their national data retention laws transposing the Directive. Starting with the Tele2 judgment in December 2016, the CJEU has issued a number of judgments about national data retention laws and their conformity with EU law. In these judgments, the Court has consistently held that laws requiring general and indiscriminate retention of all traffic data and location data for the purpose of combating (serious) crime are not compatible with the ePrivacy Directive interpreted in light of the Charter.[5]

Several Member States have amended their national data retention laws since 2014 with the objective to accommodate the CJEU case law. However, according the legal analysis done by EDRi and members of the EDRi network,[6] for most Member States the retention requirements still exceed what it permitted by EU law. This is confirmed by a recent survey of national data retention regimes by Eurojust[7] which concluded:

> *"Therefore, although some domestic laws may now meet the requirements set by the CJEU, it can be concluded that the varying efforts of Member States have not resulted in a legal framework on data retention in the EU that follows a recognisable or similar pattern."*

The call for evidence highlights that there are substantial discrepancies between the current retention requirements in Member States, and that this leads to obstacles when police and prosecutors request access to data. **The predominant explanation for the discrepancies noted by the Commission is that most national laws have excessive retention requirements compared to what is permitted by EU law. If all Member States amended their national laws to faithfully comply with the requirements set by the CJEU, the discrepancies noted by the Commission would be**

5 The complex issue of data retention for national security will not be discussed in this consultation response since the call for evidence explicitly focuses on access to data for criminal proceedings.

6 See for example, Privacy International, National Data Retention Laws, May 2024, https://privacyinternational.org/report/5267/pis-briefing-national-data-retention-laws

7 *The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU*, Eurojust and EJCN, November 2024 https://www.eurojust.europa.eu/publication/effect-court-justice-european-union-case-law-national-data-retention-regimes-judicial-cooperation

considerably reduced.

In the call for evidence, the Commission claims that as a result of these discrepancies, the necessary data is often not available or has been deleted when law enforcement requests access in the course of investigations. This framing in the call for evidence suggests that the real agenda of reducing discrepancies in Member States' retention requirements is to **increase retention requirements** for service providers.

Indeed, Council working groups since 2017 and Working Group 2 (WG2) of the High Level Group on "Access to Data for Effective Law Enforcement" (or "Going Dark", HLG) have looked for "a way forward" that would somehow allow Member States to maintain their data retention laws that originally transposed the Data Retention Directive. Eleven years after the annulment of that directive in April 2014, and despite a number of subsequent CJEU rulings holding that general and indiscriminate data retention is not compatible with EU law, the majority of Member States still have precisely that: general and indiscriminate retention requirements for traffic data and location data which allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained.

In the meantime, while putting political pressure on the CJEU to permit more data retention, **Member States ignore the Court's rulings and maintain national data retention laws that clearly violate the fundamental rights to privacy, data protection and freedom of expression.** The Commission has repeatedly refused to start infringement proceedings against Member States with illegal data retention laws.[8] **It is not an exaggeration that data retention has become a systemic rule of law crisis in the European Union.[9]**

It has been claimed that **targeted data retention** could be a way forward in compliance with the Court's rulings. However, the criteria for targeted data retention (geographical area and group of persons) as permitted by the CJEU are considered unclear by Member States. From our perspective, it is true that the use of these criteria raises many questions in terms of the respect for a wide range of human rights, including the presumption of innocence and the right to non-discrimination. Although the Court specifies that the factors should be objective and non-discriminatory, the reality of police racism and discriminatory law enforcement practices[10] makes us strongly doubt that these requirements are currently achievable.

In reality, governments have done very little to explore this option in accordance with the guidance provided by the CJEU. Belgium and Denmark have adopted legislation on targeted data retention, but the measures in both countries are in fact general and indiscriminate data retention in disguise.[11] The thresholds selected in both laws are so low that they are rendered meaningless as almost the entire population is covered by the data retention obligation. As a result, **the practical implementation of the supposedly targeted data retention regimes would literally amount to a**

8 EDRi, "European Commission will "monitor" existing EU data retention laws", 29 July 2015 https://edri.org/our-work/european-commission-will-monitor-existing-eu-data-retention-laws/
EDRi, "Europe's Data Retention Saga and its Risks for Digital Rights", 2 August 2021 https://edri.org/our-work/europes-data-retention-saga-and-its-risks-for-digital-rights/

9 POLITICO, Lawless Europe, July 2022 https://www.politico.eu/special-report/lawless-europe/

10 ENAR, "Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe", 5 November 2019 https://www.enar-eu.org/wp-content/uploads/data-driven-profiling-web-final.pdf

11 EDRi, "New Belgian data retention law: a European blueprint?", 17 November 2021 https://edri.org/our-work/new-belgian-data-retention-law-a-european-blueprint/
Jesper Lund, "The new Danish data retention law: attempts to make it legal failed after just six days", 15 June 2022 https://itpol.dk/articles/new-Danish-data-retention-law-2022

general and indiscriminate retention, which is highly likely to be overturned by the CJEU.

The "avenues to explore" in the second background document for HLG WG2, the background document for the second plenary, as well as presentations by Germany, Spain, Italy and Slovakia which have been released through a freedom of information request by Patrick Breyer[12] (with some redactions), taken together suggest that the discussions in WG2 are going in circles around the same questions which have been on the table in various Council working groups since 2017.

For EDRi, rather than introducing a new EU instrument for data retention, the Commission's primary objective should be to **ensure full compliance with fundamental rights and the extensive CJEU case law**. In most Member States, this will require repealing existing national laws with general and indiscriminate data retention requirements originating from the annulled Data Retention Directive.

2. Data retention and access to retained data are separate interferences

EDRi has noted that Council working groups on data retention since 2017 have attempted to shift the focus from retention of data to rules for access to retained data.[13] Presumably, the intention of Member States is to justify requirements for retention of data with clear and precise rules for access to that data which provide appropriate safeguards, e.g. prior authorisation by a court and limitation to certain criminal offences.

The preference for "access" over "retention" is also evident in the HLG published documents, including its recommendations of 22 May 2024:

> *"In light of these considerations, many experts stated that an EU regime should focus not only on retention, but also on access. In particular, some experts expressed the opinion that differentiating the time limits to access retained data on the basis of categories of crime should be the only criterion regulating data retention regimes, and that solutions for very targeted access be designed on the basis of other criteria. However, some other experts raised concerns how these measures would comply with the CJEU jurisprudence, as the CJEU case-law applies to both data retention and data access."*

EDRi wishes to use the opportunity of responding to the Commission's call for evidence to point out that the CJEU case law is clear on this point: requirements for retention of data and access to that retained data constitute separate inferences with fundamental rights, and both interferences must comply with the requirements of the Charter.

It is true that one of the Court's reasons for annulling the Data Retention Directive in 2014 was that the Directive did not contain any substantive and procedural conditions for access to the retained data, nor did it lay down a specific obligation for Member States to establish such conditions.[14]

12 FragDenStat, June and November Meetings of the HLEG on access to data for effective law enforcement (FOI request) https://fragdenstaat.de/anfrage/june-and-november-meetings-of-the-hleg-on-access-to-data-for-effective-law-enforcement/

13 For example the concept of "restricted data retention" analysed in this blog post: *EU Member States plan to ignore EU Court data retention rulings*, EDRi, 29 November 2017 https://edri.org/our-work/eu-member-states-plan-to-ignore-eu-court-data-retention-rulings/

14 *Digital Rights Ireland,* C-292/12 and C-594/12, paras. 61-62.

However, in subsequent rulings on data retention obligations, **the CJEU has clarified that retention of data and access to that data are separate interferences.** Whether the retained data is actually used is irrelevant for the assessment of the interference that retention of data constitutes.[15] Moreover, the CJEU has held that access to retained data may be granted only insofar as those data have been retained by a provider in a manner that is consistent with Article 15(1) of the ePrivacy Directive.[16] This means that not only must the legality of the retention requirement be considered separately from access, it is, in fact, a precondition for allowing access to the retained data.

The CJEU has interpreted Article 15(1) in light of the Charter as precluding national legislation which for the purpose of combatting crime provides for the general and indiscriminate retention of all traffic data and location data of all subscribers.[17] This means that a general and indiscriminate retention obligation for all traffic data and location data is incompatible with EU primary law (the Charter) whether it is provided for by EU secondary law (such as the Data Retention Directive 2006/24) or national law.

In its case law, the CJEU has laid down a number of requirements for access to data that have been retained pursuant to a measure under Article 15(1) of the ePrivacy Directive. First, access may only be justified by the public interest objective for which those providers were ordered to retain that data or by an objective of greater importance.[18] Second, there must be substantive and procedural safeguards in national or Union law. When access to retained data entails a serious interference, it can only be justified by the objective of combatting serious crime, and the CJEU has insisted on prior review by a court or an independent administrative body.[19]

The recent "HADOPI judgment", which allows access to retained data about source IP addresses for ordinary criminal offences, does not depart from these principles because the CJEU explicitly requires that the general and indiscriminate retention of source IP addresses is organised in a technical manner so that the retention itself does not constitute a serious interference with fundamental rights.[20] The HADOPI judgment is analysed in further detail in section 5 of this consultation response.

As noted above, the CJEU case law has clearly established that a general and indiscriminate retention obligation for the purpose of combatting crime is contrary to EU law (the Charter) when the retained data taken as a whole allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, e.g. their location and physical movement, their social relationships and their social environments.[21] Even a short retention period cannot change this.[22] For this type of data, only targeted data retention requirements or quick-freeze measures are compatible with EU law.

For certain types of traffic data, the CJEU has clarified that a general and indiscriminate retention obligation can be compatible with EU law. Notably, general and indiscriminate retention of source IP addresses for a limited time period is allowed for the purpose of combatting serious crime, and,

15 *La Quadrature du Net and Others I*, C-511/18, C-512/18 and C-520/18, paras. 115-116
16 *La Quadrature du Net and Others I*, C-511/18, C-512/18 and C-520/18, para. 167 and *Prokuratuur* C-746/18 para. 29
17 *Tele2*, C-203/15 and C-698/15, para. 107.
18 The case law of the CJEU has established a hierarchy of national security, serious criminal offences and all criminal offences for the purposes of retention of data and access to retained data.
19 *Prokuratuur*, C-746/18, paras. 51-54
20 *La Quadrature du Net and Others II*, C-470/21
21 Tele2, C-203/15 and C-698/15, para. 107 read together with para. 99.
22 *Prokuratuur*, C-746/18, para. 40

concerning all criminal offences, only under additional conditions such as watertight technical separation (the HADOPI judgment analysed below).

However, **these data types (source IP addresses and civic identity data) must still be considered specific and narrow exceptions from the overarching principle established by the CJEU case law** since 2014 that general and indiscriminate retention of traffic data and location data for the purpose of combatting criminal offences is not compatible with EU law. In particular, the CJEU rulings on retention of source IP addresses cannot necessarily be directly extended to retention of assigned source IP addresses and port numbers.[23]

From the recommendations of the HLG and various Council documents, EDRi understands that Member States find the concept of targeted data retention difficult to implement. Albeit for other reasons, EDRi is also critical of targeted data retention because the criteria suggested by the CJEU raise many questions in terms of the respect for a wide range of human rights, including the presumption of innocence and the right to non-discrimination, as noted in section 1 of this consultation response.

EDRi would therefore recommend that a future EU instrument on ensuring access to data for law enforcement focuses on quick-freeze options rather than mandatory data retention. Quick-freeze orders can be targeted to particular criminal investigations and are less susceptible to risks of discrimination and undue interferences with the presumption of innocence.

3. There is no reliable evidence that mandatory data retention is necessary

3.1. The availability of data is greater than ever due to dominant business models

In the political context and problem definition, the Commission remarks that to effectively fight crime, law enforcement and judicial authorities may need access to certain non-content data processed by electronic communication service providers. In the absence of specific data retention obligations, this data may be deleted by the time authorities request access to the data.

The problem is presented as if increased data access by law enforcement in itself is an objective of general interest – which is not the case - and that the current situation systematically prevents law enforcement authorities from carrying out their tasks.

The background document for the second HLG plenary meeting highlights the difficulties in providing statistics which could quantify the importance of lawful access to data.[24] However, EDRi has repeatedly pointed out that this failure by EU institutions and Member States' authorities to

23 This issue still requires clarification by the CJEU, as pointed out by the Advocate General in point 83 of the Opinion on *SpaceNet and Telekom Deutschland*, C-793/19 and C-794/19.

24 "Despite requests to this end, it appears unfeasible for law enforcement authorities to classify the criminal case types that are more or less reliant on access to data to be solved, as well as the categories of data which are necessary to investigate and prosecute criminal offences. National experts highlighted the difficulties faced in providing statistics which could quantify the importance of lawful access to data for successfully investigating and prosecuting crime, regardless of the type of offence suspected or the type of data required", Input to the second plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement, 21 November 2023 https://home-affairs.ec.europa.eu/document/download/05963640-de76-4218-82cd-e5d4d88ddf96_en?filename=HLG-background-document-21112023.pdf (page 2)

provide evidence about the marginal benefits of access to electronic data compared to less intrusive alternatives leads to legislative proposals which do not satisfy the test of necessity.[25]

In the discussions on data retention for the past two decades, governments have claimed that absence of general and indiscriminate data retention (mass surveillance) has a negative effect on law enforcement's ability to combat crime. However, evidence to support this claim has never been presented. **There is no measurable effect from data retention on crime rates or crime clearance rates in EU Member States.[26]** A study conducted by the Max Planck Institute for Foreign and International Criminal Law in 2012 found that blanket data retention requirements did not lead to higher crime clearance rates.[27]

In November 2020, the Commission published a study on data retention[28] which regrettably only collected evidence from law enforcement and service providers, omitting civil society organisations and other critical stakeholders.[29] Despite the narrow focus on law enforcement and commercial interests, which are likely to bias the study in favour of data retention, the study does not present any evidence which could support a claim that mandatory data retentions meets the threshold of necessity. Whilst there are differences across the 10 Member States surveyed (three of which do not have data retention laws), **the overall conclusion of the study is that all types of non-content data are retained by electronic communications service providers (ESPs) for at least one internal purpose** (e.g. invoicing marketing, and network security).[30]

The provision of evidence is critical for assessing the necessity and proportionality of the policy options considered by the Commission for future EU rules on data retention. However, we still don't see the Commission seriously taking this requirement into account in its call for evidence.

3.2. The permanent failure to provide evidence affects compliance with the necessity requirement

With the pervasive use of online services and smartphones, and the predominant business model of surveillance capitalism which leads to massive data collection for commercial purposes (e.g. behavioural advertising and training large AI models), **law enforcement is literally enjoying a golden age of surveillance with access to more data about European residents than ever before.** Before mobile phones became ubiquitous, people didn't carry electronic devices which allow law enforcement to track the physical movement, social networks, preferences and habits of everyone. This, by itself, should call into question the necessity of proposals for general and indiscriminate data retention. Such measures constitute particularly serious interferences with the fundamental right to privacy and data protection, as well as other fundamental rights, and they generally fail to

25 EDRi, Data Retention Revisited, 2020 https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf

26 EPRS, General data retention / effects on crime, 5 October 2020 available at: https://www.patrick-breyer.de/en/study-data-retention-has-no-impact-on-crime/?lang=en

27 Max Planck Institute for Foreign and International Criminal Law, "Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten" [Security gap due to the absence of data retention? An investigation into security and law enforcement issues in the absence of telecommunications metadata storage], July 2011, available at: https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf;
For an English summary see: https://www.vorratsdatenspeicherung.de/content/view/534/79/lang,en/.

28 European Commission: Directorate-General for Migration and Home Affairs, Milieu, Dupont, C., Cilli, V., Omersa, E. et

29 *Blanket data retention: biased study by the EU Commission*. Digital Courage, 18 March 2020 https://digitalcourage.de/blog/2020/data-retention-biased-study-by-the-eu-commission

30 EC data retention study, page 58

meet the legal requirements for necessity and proportionality in Article 52(1) of the Charter of Fundamental Rights.

3.3. Less intrusive alternative methods are equally efficient to achieve the same objective

Most law enforcement requests for non-content are successful, even in Member States without a data retention law. According to the 2020 Commission study, only slight variations can be detected between LEA (law enforcement authority) survey respondents from Member States with and without mandatory data retention. The retention periods for non-content data are invariably shorter in Member States without mandatory data retention, but **the German police have managed to adapt to the shorter retention periods by obtaining judicial approval for access requests within a week.**[31]

Digital rights organisations have consistently opposed mandatory data retention and instead proposed less intrusive methods such as quick freeze (also called "preservation orders"). A preservation order is restricted to the data that would assist in a particular investigations, and does not lead to general and indiscrimination data retention for long periods of time. In the study, LEA survey respondents give a negative view of quick freeze which provides less flexibility than retention and is more cumbersome because two authorisations are required, one for preservation and one for the subsequent access.[32] However, **none of these objections from LEA respondents come even close to demonstrating the necessity of mandatory data retention over the less intrusive preservation orders. We would like to stress that "convenience" and "efficiency" are (still) not legitimate grounds to unduly restrict fundamental rights under the Charter. The lack of necessity is further reinforced by the fact that the success rate for law enforcement data access requests depends very little on whether there is a mandatory data retention regime or not.**

The study mentions that national rules on quick freeze often restrict the use of the tool to certain types of non-content data, while mandatory data retention covers a broader selection of non-content data.[33] However, **there is no legal reason that the less intrusive instrument (quick freeze) should be used more restrictively than general and indiscriminate data retention.** On the contrary, quick freeze should be more readily available for law enforcement than mandatory data retention, as long as the use of the quick freeze instrument is targeted to specific investigations in a non-discriminatory manner, respects the principles of necessity and proportionality and comply with all the applicable EU and national procedural safeguards. In any case, this is a limitation that Member States should be able to address in their national laws in compliance with fundamental rights. Conceivably, **the Member States in question have failed to adequately develop their quick-freeze provisions because they prefer mandatory data retention**, and thus far they have been able to ignore the rulings from the CJEU that EU law precludes general and indiscriminate data retention (of all traffic data and location data).

3.4. The reality of cross-border cases does not call for harmonised data retention rules

Cross-border access to non-content data is frequently invoked as a rationale for harmonising data retention requirements in Member States. A cross-border access request may be unsuccessful if the data is deleted before cross-border access request procedures are completed. Currently, law enforcement must use either mutual legal assistance (MLAT) procedures or the European

31 Ibid page 65
32 Ibid page 96
33 Ibid page 97

Investigation Order. The delays with these instruments are highlighted in the 2020 EC data retention study. However, from August 2026, the e-Evidence Regulation will enter into application. EU law enforcement authorities will be allowed to send legally binding production and preservation orders to service providers established or represented in another Member State.

We would like to point out that the e-Evidence Regulation was repeatedly criticised by civil society, internet service providers and professional organisations for their lack of sufficient safeguards and the circumvention of important rules in existing international cooperation frameworks (e.g. MLATs).[34] This notwithstanding, we do recognise the potential for faster cross-border procedure[35], which should address the concerns raised by LEAs in the 2020 EC study, In any case, **it is (obviously) still too early to early to assess if the e-Evidence framework is effectively leading to too many rights infringements or if it is insufficient in addressing some of the law enforcement claims.**

As emphasised in section 1, the predominant explanation for the discrepancies in data retention requirements between Member States (observed by the Commission in the call for evidence) is that most Member States have broader data retention requirements than what is permitted by the CJEU case law.

4. Data retention for OTT (number-independent) providers threatens the right to anonymity online

The call for evidence, along with the published documents from the HLG. reveals an interest in extending data retention laws to providers of number-independent interpersonal communications services (hereafter: OTT (Over the Top) providers), which since December 2020 are part of the ePrivacy data protection regime.

4.1. Legal, jurisdictional and technical obstacles to data retention for OTTs

Although the CJEU has not ruled on data retention for OTT providers, **it must be assumed by analogy that a general and indiscriminate retention obligation for all EU users is prohibited by the ePrivacy Directive and the Charter.** Only targeted retention can be compatible with EU law, at least insofar as the retention obligation applies to metadata (traffic data and location data), which allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, e.g. their location and physical movement, their social relationships and their social environments.[36] This includes any metadata about actual private communications (sender, recipient, time of communication) and any location data collected by the service provider.

Most number-independent services are offered globally through the internet (OTT) by companies

34 EDRi, e-Evidence compromise blows a hole in fundamental rights safeguards, 7 February 2023, https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/

35 At the time of the discussions on the adoption of new EU and Council of Europe instruments for cross-border access to data by law enforcement, MLATs were misrepresented as being categorically unsuitable for dealing with electronic evidence because they are too slow. Several digital and human rights organisations had therefore advocated for improving the MLATs system, for example by introducing stricter deadlines and allocating more resources to judicial authorities to process requests. The new regime of "direct orders" (sent directly to service providers in another jurisdiction) constitutes a short-cut for law enforcement taking out several basic human rights safeguards, and shifting the burden to service providers (which do not have the same human rights obligations that States do). See for example: https://edri.org/files/consultations/globalcoalition-civilsocietyresponse_coe-t-cy_20180628.pdf

36 *Tele2*, C-203/15 and C-698/15, para. 99

with a main establishment outside the European Union. **The providers may not technically be able to comply with a data retention obligations for some of their European users. They certainly cannot be expected to introduce a global data retention scheme through their terms of service in order to comply with national law in a given EU Member State or Union law for that matter.**

The background documents of the HLG point out that some OTT providers retain no data at all. This is to be expected given the increased global focus on privacy, the advantages of anonymous communications, and the risks associated with storing personal data (e.g. data breaches). These are the same drivers that lead people to prefer secure end-to-end encrypted (E2EE) communications services over cleartext services, where their private communications and associated metadata can be monitored by private companies and state actors.

Some E2EE communication services apply concepts such as "sealed sender" that technically prevents even the service provider from monitoring who is communicating with whom. This technical design supports key principles in EU data protection law, notably data protection by design in Article 25 of the GDPR and the main rule in the ePrivacy Directive that users' communications and data relating thereto will remain anonymous and may not be recorded.[37] However, **this also means that a data retention obligation for metadata is technically impossible due to the design of service.** In this connection, it should be recalled that the scope of the Data Retention Directive was traffic data generated or processed by the provider, which refers to data that is actually accessible to the provider.[38] The Data Retention Directive did not contain an obligation to generate additional data for the sole purpose of retaining it.

E2EE communication services with technical concepts such as "sealed sender" effectively apply encryption to metadata used for provision of the service in order to protect that metadata from the risk of abuse, including data breaches and cyberattacks against the service. **A legal obligation to make that metadata available for retention requirements, including a targeted retention obligation, would involve a general weakening of the security of that communications service affecting all users of the service.** This can be directly compared to a backdoor requirement in order to facilitate the interception of the content of communications for some users in a targeted manner. The security of all users is adversely affected and, very likely, critically undermined.

In Podchasov v. Russia, application no. 33696/19, the European Court of Human Rights (ECtHR) held in para. 79 that national legislation which weakens the encryption mechanism for all users is not proportionate to the legitimate aim pursued under Article 8 of the European Convention of Human Rights. Whilst the ECtHR case is about technical backdoor measures to facilitate interception of the content of electronic communications, **the same principles should apply, by analogy, to interception or retention of metadata for electronic communications (traffic data)**, as both courts (CJEU and ECtHR) have held that metadata provides the means of establishing a profile of the individuals concerned, information that is no less sensitive or intrusive, having regard to the right to privacy, than the actual content of communications.[39]

In summary, while a data retention obligation in compliance with the case law of the CJEU could, in principle, be extended to number-independent services (OTT providers), there will be a number of legal, jurisdictional and technical obstacles that are likely to render the proposal infeasible in practice.

37 *La Quadrature du Net and Others,* C-511/18, C-512/18 and C-520/18, para. 109
38 Recital 13 of the Data Retention Directive 2016/24/EC (annulled)
39 *Tele2*, C-203/15 and C-698/15, para. 99 and *Big Brother Watch and Others v. the United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15), para. 363

4.2. The crucial need for and right to anonymity online

As civil society organisations, we seriously question the necessity of additional data retention obligations for OTT services when most of these services already collect a substantial amount of personal data for their commercial purposes, especially the predominant Big Tech services. As of August 2026, the e-Evidence Regulation will enable law enforcement authorities in Member States to issue cross-border production and preservation orders directly to service providers offering services in the EU.

There are a limited number of privacy-focused services with E2EE and no metadata collection for commercial purposes which are likely to employ anonymity-by-design technologies that make metadata collection technically impossible. **Extending data retention requirements to such providers would force them to choose between offering the services they market—secure and private communications—while refusing to comply with the law, or pulling their services out of that particular Member State's market.** There is no technical way to create a door (or a pool of retained data) that opens for the "good" law enforcement actors but not malicious, bad actors.[40]

Pressuring security-focused providers of electronic communications services into weakening the security of their service would **undermine not only the security of their users, but also the rights to privacy, data protection, and other fundamental human rights enshrined in the EU Charter.** The lack of a forum to enjoy secure, private communications free from government scrutiny chills individuals' free speech, free expression, freedom of thought, and freedom of assembly.[41] Being able to develop, offer and choose trustworthy communication systems is essential in democratic societies, particularly in light of highly intrusive interceptions of communications by (non-)state actors and increasingly shrinking civic space in the EU.[42] Most likely, security-focused providers established outside the EU would simply refuse to do so, similar to their refusal to comply with national laws requiring encryption backdoors.[43]

40 For example, the built-in vulnerabilities of TLS/SSL protocols affected government websites for a decade before being patched in 2015: https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa/. Other examples include the hack of the lawful interception facilities of Vodafone in Greece called "The Athens Affair" which enabled the eavesdropping of over 100 politicians, with serious consequences for national security: https://spectrum.ieee.org/the-athens-affair. Another recent example is the massive cyberattack that penetrated United States broadband networks, including AT&T and Verizon, through the channels used by the United States government to engage in court authorized broadband network wiretaps: https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b

41 See, e.g. see also Jeramie D. Scott, Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space, 12 J. Bus. & Tech. L. 151 (2017), https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2 (discussing the chilling effects of government surveillance on private communications).

42 Bill Marczak & John Scott-Railton, *First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted*, Citizen Lab (June 12, 2025), https://citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/

43 For example, Signal clearly announced that it would exit the UK market when a bill opened the door for the government to require client-side scanning, see https://signal.org/blog/uk-online-safety-bill/

5. Assessment of the CJEU case law for retention of IP addresses (HADOPI judgment): technical solutions cannot prevent serious interference with the right to privacy in all circumstances

This section is adapted from an EDRi blog post which analyses the HADOPI judgment[44] and considers its implication for the ongoing political debate on the mandatory retention of traffic and location data (metadata) by internet companies for access by law enforcement authorities.[45]

The main conclusion of EDRi's analysis is that whilst the CJEU does allow retention of and access to source IP addresses for all criminal offences in the new judgment, this is done under conditions that seem tailor-made to the functioning of HADOPI system, and may not realistically exist outside the HADOPI system which has very specific rules for processing personal data. **EDRi therefore cautions against relying on the HADOPI judgment to design future polices for retention of metadata for internet service providers.**

5.1. The degree of interference of IP addresses retention

The Court re-assesses the seriousness of the interference with fundamental rights of the retention and access to IP addresses associated with a user's civil identity (LQDN II, para. 79-84). In its La Quadrature du Net and Others judgment[46] from October 2020 (LQDN I), the Court held that the general and indiscriminate retention of source IP addresses is a serious interference with the rights to privacy, data protection and freedom of expression, and thus can only be justified by the objective of fighting serious crimes (LQDN I, para. 156). It was considered a serious interference because it allows to "track an internet user's complete clickstream" and draw precise conclusions about their private life (LQDN I, para. 153).

In LQDN II, the Court clarifies that retention of source IP addresses is not a serious interference if the national legislation mandates technical retention arrangements which rule out that precise conclusions about the private life of the person can be drawn. This requires watertight separation between IP addresses, civil identity data and other traffic data and location data. The only exception to the complete separation of data categories is when IP addresses and civil identity data are linked, and this must be done through an effective technical process that does not undermine the watertight separation.

In essence, the Court envisages a closed retention system where personal data can only be extracted from the "black box" by querying the system for the civic identity data associated with a specific source IP address at a specific time. By conceptually precluding a serious interference through technical means, the Court paves the way for retaining IP addresses the purpose of fighting all offences, including relatively minor ones like copyright infringement. This elaborate reinterpretation of the extensive case law very conveniently saves the HADOPI system.

It is unlikely that current retention practices by internet service providers conform to the detailed requirements about watertight separation set out by the Court. The elephant in the room is whether Member States will actually amend their data retention laws and enforce the new security

44 *La Quadrature du Net and Others*, C-470/21 ("LQDN II")

45 *CJEU saved the HADOPI: what implications for the future of data retention in the EU?* EDRi, 3 April 2025 https://edri.org/our-work/cjeu-saved-the-hadopi-what-implications-for-the-future-of-data-retention-in-the-eu/

46 *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18 ("LQDN I")

requirements. Data retention laws in many Member States already allow access to retained IP addresses for all criminal offences – which was in contradiction with the CJEU's previous case law. **It is not inconceivable that these Member States will simply see the HADOPI judgment as vindication for their current laws and tacitly ignore the watertight separation requirements that are critical in the judgment.**

5.2. The degree of interference of IP addresses access

It is already established case law that access to retained data for the sole purpose of identifying a user does not constitute a serious interference when it is not possible to associate that data with information about the communications made (LQDN I, para. 158). However, in the context of identifying an internet user there is an inherent link to the communications made. Law enforcement may have additional information which can reveal intimate details about the person concerned and make the interference a serious one.

In 2018, in Benedik v. Slovenia,[47] the European Court of Human Rights (ECtHR) rightly mentioned how data sought by the police (namely the name and address of a subscriber) combined with pre-existing content (the content shared online) is capable of revealing "a good deal about the online activity of an individual, including sensitive details of his or her interests, beliefs and intimate lifestyle" (Benedik v. Slovenia, para. 109).

Yet, the CJEU considers that such situations are "atypical" in the case of HADOPI because the information available to HADOPI, such as the type of copyrighted content and the file name, is limited and rarely reveals sensitive information (LQDN II, paras. 111-112). It adds that only a limited number of public officials accesses the data (LQDN II, para. 113) and are bound by a confidentiality obligation (LQDN II, para.114) which prohibits any disclosure of information to other parties, except for referring the case to the public prosecutor in stage 3.

These arguments about potentially sensitive information being strictly contained can be seen as "tailor-made" to the HADOPI system. This also means that they will not necessarily apply to other types of investigations. In fact, even in the case of HADOPI, the Court recognises later in the judgment that the third stage may involve a serious interference because precise conclusions about the person could emerge from the linking of information from all three stages (LQDN II, para. 141).

Lastly, the Court states that fundamental rights protection cannot go as far as "making it impossible or excessively difficult" to prosecute online offences (LQDN II, para. 116). With that reasoning, the Court takes over the Advocate General's argument of a substantial risk of "systemic impunity" online. The fundamental rights to privacy and protection of personal data are not absolute, but the principle of proportionality must put limits on how much personal data can be processed, especially for minor offences. **EDRi has repeatedly pointed out that given the surveillance-based advertising business model of most online services nowadays, more information is available for investigative purposes than ever before.**

5.3. Implications for future data retention policies

It is doubtful whether this ruling actually clarifies the legal situation for IP address retention and access. The Court allows data retention of IP addresses for combatting minor offences and access to that data without prior authorisation by a court. This is done under conditions that seem tailor-made to the functioning of HADOPI system, and may not realistically exist outside the HADOPI

47 Benedik v. Slovenia, application no. 62357/14, ECtHR, 24 April 2018

system which has very specific rules for processing personal data.

In the broader context of law enforcement investigations seeking to identity internet users from their IP address, the judgment says that this access can be a serious or non-serious interference, and that prior authorisation by a court is sometimes needed. This leaves a lot of ambiguity, which the judgment only settles for the HADOPI system.

The conditions that make the third HADOPI stage special, notably the connection to the context of the internet behaviour under investigation, are really the typical case in almost all other investigation where law enforcement seeks to identify internet users. From a digital rights perspective, that would be a positive reading of the HADOPI judgment, emphasising the critical importance of context as in Benedik v. Slovenia.

In a context of relentless attacks against human rights defenders, journalists and NGOs, the ability to protect one's privacy online through anonymity is of paramount importance. We recommend the Commission and the EU legislators to maintain high protection standards in any future legislation and to provide a clearly defined framework for data retention and access which leaves no discretion to law enforcement to define the level of interference with rights and what procedural safeguards should apply.

6. Data retention of source IP addresses and port numbers may lead to potentially serious interference with the right to privacy

The HLG recommendations include a harmonised EU regime on data retention covering *inter alia* source IP addresses and port numbers for electronic communications services that provide internet access (ISPs). EDRi understands that **the purpose is to identify the subscriber when Carrier-Grade Network Address Technology (CG-NAT) is used by the ISP**. With CG-NAT, the same public IPv4 address can be used by a large number of subscribers at the same time which may present obstacles to law enforcement investigations.

In principle, the combination of a shared IP address and a port number uniquely assigned to the subscriber can be compared to the circumstances considered by the CJEU in the HADOPI case analysed in the previous section. The (shared) source IP address and port number do not, as such, disclose any information about communication with third parties. **However, linking the source IP address and port number with other information may give rise to a potentially serious interference with the right to privacy.**

Despite the apparent similarity with the HADOPI case, there are a number of important differences when port numbers are retained as well. **The retained data, taken as a whole, will reveal more details about the private life of the person concerned. This means retention of port numbers constitute a greater interference with fundamental rights than retention of only IP addresses, as outlined in the following.**

First, the amount of data retained will increase massively, along with the costs for ISPs. A source IP address is a single record covering a session (time period) with connectivity to the internet for the user. On the contrary, different source ports in CG-NAT scenarios are assigned for every connection where internet packets are exchanged with a server. **A simple website visit can involve as much as 200 different connections of short duration to handle the elements embedded on a website,**

especially if online tracking and programmatic advertising is involved. The simple website visit will lead to 200 NAT session records being retained.[48]

The intensity (frequency) of those NAT session records can by themselves reveal detailed information about a persons life, especially for a residential internet connection, for example behavioural pattern during day (sleeping patterns and whether the person is at home or not). **In terms of intrusiveness, this can be compared to the serious privacy concerns about smart meters.**

Second, the massive increase in retained data records will only be useful to the police if online services also register the source port used along with the IP address. The experience of the Danish National Police shows that **social media platforms often do not log port numbers**.[49] This limitation casts considerable doubt on the necessity of requiring ISPs to retain port numbers for CG-NAT session.

Finally, **the retention of source port numbers lead to a much greater risk that users are incorrectly singled out for police investigations based on flawed evidence.** When the police requests civic identity data of a user, the ISP must match an IP:port:timestamp combination from the police to its own retained data. This process is very susceptible to errors in the timestamp synchronisation between the internet service provider and the online platform (website). **A mismatch of just a couple of seconds can easily lead to the wrong person being suspected.** Whilst this problem also exists for retention of just source IP addresses, for example when incorrect time zones are used for one of the recorded timestamps,[50] **the severity of the problem will increase considerably when port numbers are also involved in the information needed for identifying a user.**

48 A NAT session record consists of a source IP address, source port number, as well as the start and end timestamp for the session where this IP:port combination was assigned to the user (subscriber).

49 Briefing note from the Danish National Police distributed by the Ministry of Justice to The Legal Affairs Committee, 4 August 2021 https://www.ft.dk/samling/20201/almdel/REU/bilag/399/2434065.pdf

50 *The Wrong Internet Address: Police Data Errors and Arrests*, Iain Gould, 16 July 2020 https://iaingould.co.uk/2020/07/16/the-wrong-internet-address-police-data-errors-and-arrests/