

# CCBE response to the public consultation on the impact assessment on retention of data by service providers for criminal proceedings

September 2025

---

*The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 46 countries, and through them more than 1 million European lawyers. The CCBE is recognised as the voice of European lawyers, representing European Bars and Law Societies in their common interests before European and other international institutions. Defending human rights and the rule of law are central values of the CCBE.*

## Introduction

1. The CCBE welcomes the opportunity to provide its feedback in this public consultation and would like to offer its expertise and readiness for future engagement in the planned impact assessment on the proposed measure on data retention.
2. At the same time, the CCBE would like to express our concern about the timing and the quality of the public consultation questionnaire. Concerning the timing, the CCBE is convinced that a consultation of such importance should not be carried out over the summer period where many organisations, ours included, need sufficient time to consult their membership in order to provide an up-to-date and representative feedback. Concerning the quality, the CCBE found the questions in the survey questionnaire biased and too general to be able to provide a sufficiently nuanced picture of the current practices in the field of data retention and the practical application of the existing investigatory measures in the EU. This is all the more important given the differences in national criminal laws and criminal procedural laws. The CCBE notices that the responses to the questions formulated as they are now will give a wrong picture of the issue at hand and the challenges associated therewith.
3. For example, the questions about the lack of digital evidence or the lack of relevant rules or obligations are too general and at the same time ask about several things. Any answer, positive or negative, would require several qualifications and further nuance. For example, there are already several EU-level investigative measures allowing for requesting relevant electronic evidence, including metadata. However, their practical application may differ from one context to another. Therefore, a simple yes or no answer would not provide a sufficiently nuanced and comprehensive picture which in our view is indispensable for an impact assessment.
4. The CCBE would like to point out that it is impossible for it to answer the question on retaining metadata for longer periods and retaining additional types of metadata. The question concerns two things at the same time and concerns different subjects: one is about the retention schedule and another is about the types of data to be retained. Any answer would offer a wrong interpretation of the current needs and challenges.

5. It is also impossible to answer the question on whether metadata should be accessed only in case of serious crimes or other types of crimes as well. This is because there is no definition of what serious crime is on the EU-level, as in other legal instruments regarding data retention, the definition of this notion is left to the Member States, insofar this definition is in accordance with Union law (e.g. CJEU 30 April 2024, nr. C-178/22, *Bolzano*, para 44-47). Moreover, the access and subsequent use of data are specific to concrete investigations and their circumstances.
6. The question about the risks to fundamental rights does not seem to cover risks to the right to a fair trial and to the violation of the principle of professional secrecy/legal professional privilege.
7. In the CCBE's view, the question about ranking various investigative methods according to their level of risk is way too general to be able to make such a decision and from our point of view does not add any informative value to the outcome of the consultation. The question about measures which would be less intrusive and still allow for the effective investigation and prosecution of crimes is also too general. The CCBE is actually concerned how the results might be interpreted ahead of the preparatory work to the proposed legislative instrument. Finally, the CCBE is not sure why options such as 'house search' or 'seizure of devices' were added in the context of a consultation on retention of metadata by communications services providers. The CCBE would like to underline, that both law and case law provide that the proportionality of a measure is to be assessed on the basis of its circumstances. The questions in the questionnaire do not reflect this legal requirement.
8. Finally, the question on retention of data according to the type of investigation seems to concern the situation in which different types of data are stored for different purposes. In practice, however, all data would have to be stored for the same amount of time until a relevant request is made by the relevant law enforcement authority.
9. It is for these reasons that the CCBE decided not to provide our responses via the questionnaire but instead chose to offer its remarks and recommendations in this paper.

### **General remarks**

1. The CCBE understands the evolving nature of the challenges facing law enforcement authorities (LEAs) in their activities to prevent, detect and investigate criminal activity, especially given the pace of technological advancements and the fact that a large proportion of criminal activity has a digital footprint. The CCBE fully supports the objectives to combat crime and the adoption of specific measures to prevent and fight it.
2. At the same time, the CCBE would like to stress once again that new, and sometimes expanded, powers of law enforcement authorities – should they be deemed to be desirable and legally proportionate – must be accompanied by appropriate safeguards against abuse, especially in situations where the legal frameworks and traditions of various jurisdictions differ from one to another.
3. The CCBE is particularly concerned by potential threats regarding law enforcement access to data which can interfere with the fundamental right of confidentiality of lawyer-client communications, and other fundamental rights such as the right to privacy, the right to a fair trial and the right to be advised, represented and defended by a lawyer. This adds an additional layer of complexity with regard to cross-border crime or cross-border investigations, especially with regard to obtaining electronic evidence.
4. Likewise, the CCBE is also concerned about the potential impact on the right to defence and to a fair trial including the presumption of innocence or the principle of equality of arms. To this end,

the CCBE included several observations and recommendations which it hopes will assist the Commission in its work on the impact assessment and, if applicable, on the proposed legislative measure.

### **Importance of professional secrecy/legal professional privilege**

1. The protection of professional secrecy/legal professional privilege (PS/LPP) is a fundamental right and the foundation of the proper administration of justice and the right to a fair trial. It has been extensively recognised as such in the case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the EU (CJEU). In particular, the ECtHR states in *Michaud* that: *'[...] while Article 8 protects the confidentiality of all "correspondence" between individuals, it affords strengthened protection to exchanges between lawyers and their clients. This is justified by the fact that lawyers are assigned a fundamental role in a democratic society, that of defending litigants. Yet lawyers cannot carry out this essential task if they are unable to guarantee to those they are defending that their exchanges will remain confidential. It is the relationship of trust between them, essential to the accomplishment of that mission, that is at stake. Indirectly but necessarily dependent thereupon is the right of everyone to a fair trial, including the right of accused persons not to incriminate themselves.'*<sup>1</sup>
2. The ECtHR thus affords a strengthened protection under Article 8 of the European Convention on Human Rights (ECHR) to communications falling within the protection of PS/LPP as a fundamental right. Moreover, the CCBE would like to recall that although the Article 8 right is qualified, the right to a fair trial according to Article 6 ECHR is absolute and not a qualified one. Therefore, if a legally privileged communication, or a communication protected by an obligation of professional secrecy does fall within the scope of Article 6 ECHR, then, given the absolute nature of the protection afforded by this article, there should be no possibility of accessing such communications.
3. There are several situations where the data retained by communication services providers (and others) may be covered by PS/LPP when seized by law enforcement authorities (LEAs): data belongs to a lawyer or a law firm and/or data belongs to a person who is a suspect or an accused person and they communicate with their lawyer. There are numerous practical impacts and risks of the obligation of indiscriminate data retention on lawyers and their clients. Taken together and analysed, metadata provides ample information for pattern analysis that can reveal considerable detail of the nature of the lawyer's activities and the relationships with their clients. This includes:
  - tracking repeated communications between lawyers and their clients;
  - identifying location patterns showing when and where meetings occur, as well as how long they last, the intervals at which they take place, etc.;
  - establishing timelines of lawyers' activities;
  - mapping lawyers' professional networks and associations;
  - identifying all parties a lawyer communicates with;
  - identifying potential topics or content of legal advice (e.g. through browser history data or app usage metadata);
  - identifying clients (in some jurisdictions it is part of PS/LPP);
  - mapping professional relationships within law firms; or
  - monitoring patterns that might indicate specific types of legal work or working in specific geographical areas.
4. An unbridled and unbalanced application of these technological possibilities would definitely impact the right to defence and the right to a fair trial.

---

<sup>1</sup> [Para 118, Case of Michaud v France, Application No 12323/11](#)

5. A concrete example may be illuminating in this regard:

*Suppose a person fears prosecution for committing an act that might have been punishable under criminal law. Therefore, they seek advice. They contact a lawyer by phone and request advice. Due to the complexity of the case, the client and the lawyer exchange calls several times throughout the day, and the lawyer ultimately advises the client that, in his opinion, no crime was committed.*

*Later, a judicial investigation is initiated, with a competent judicial authority issuing a warrant ordering the suspect's identity, traffic, and location data to be produced.*

*The results of this production order show that shortly after the facts under investigation, the suspect had contacted a lawyer by phone on several occasions. This information is then used by the police and judicial authorities to suggest that the suspect apparently needed legal assistance at that time because, hypothetically, he knew he had committed a crime.*

*The result is clear: obviously, both the suspect and others seeking legal assistance will think twice before consulting a lawyer and asking for their advice.*

*Therefore, it is clear that there is a risk of a chilling effect of unbalanced and unbridled possibilities for data retention and consultation of that data on the rights of defence and the right to a fair trial in general, and the actual confidentiality of communications between a lawyer and their client in particular.*

6. Likewise, the impact on the right to privacy is obviously at stake.
7. The above is all the more important since, following several CJEU judgments and the requirement that retention of data must be targeted<sup>2</sup>, many EU member states allow such retention albeit to varying extents. Taking the example of geographical limitations, in some countries data may be retained in such locations as airports or major train stations, which are used by lawyers, among others. Moreover, depending on their areas of practice, some lawyers may regularly travel to areas that have been determined as having a higher crime rate. In addition, even if lawyers are not subject to such surveillance measures, their clients may and thus their lawyers can be identified. Also, there are wider and more general implications of the geographical restriction on all people that are present in certain areas and thus their rights may be infringed.

#### **Relevant EU-level case law relating to metadata**

1. In *Digital Rights Ireland* (8 April 2014, C-293/12, C-594/12), the Court found that the blanket retention of traffic and location data “is liable to generate in the minds of the persons concerned [...] the feeling that their private lives are the subject of constant surveillance” (para. 37). It stressed that metadata, taken as a whole, “may allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained, such as habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them” (para. 27). Thus, the Court recognised metadata retention as a particularly serious interference with privacy, not merely a minor intrusion.
2. In *Tele2 Sverige* (21 December 2016, C-203/15, C-698/15), the Court reiterated that **metadata enable very precise conclusions** about private life “such as everyday habits, places of residence, movements, activities, social relationships, and the social environments frequented” (paras. 99–

---

<sup>2</sup> See for example: C-140/20, *Commissioner of An Garda Síochána and Others*, [ECLI:EU:C:2022:258](#)

100). Even without access to communication content, retention of metadata “may be considered to be particularly serious” (para. 100). On that basis, the Court held that **general and indiscriminate retention** of traffic and location data is disproportionate and precluded by Art. 15(1) ePrivacy Directive and the EU Charter of Fundamental Rights.

3. In *Ministerio Fiscal* (2 October 2018, C-207/16), the Court stated that access to **civil identity data** (e.g., identifying the subscriber behind a dynamic IP) **does not, in itself, constitute a “serious” interference** requiring the serious-crime threshold, provided access is necessary and proportionate and framed by clear and precise rules; nonetheless, access remains an interference that must be **law-based** and with appropriate **safeguards**.
4. In *Privacy International* (6 October 2020, (C-623/17), the Court held that measures requiring providers to transmit/retain traffic/location data for national security fall within the scope of the ePrivacy Directive when they compel private providers, and Article 15(1) of Directive 2002/58, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights precludes any national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.
5. In *La Quadrature du Net and Others* (6 October 2020, C-511/18, C-512/18, C-520/18), the Court again highlighted the **sensitive nature of metadata**, noting that general retention “is likely to allow very precise conclusions to be drawn concerning the private life of the persons whose data are retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them” (para. 117, quoting Digital Rights Ireland and Tele2). The Court also linked metadata retention with **chilling effects** on freedom of expression (Art. 11 Charter).
6. The Court ruled that the retention of metadata is permitted **only exceptionally** (strictly limited in time and scope, and subject to strong safeguards).
7. In *Prokuratuur* (2 March 2021, C-746/18), the Court reaffirmed that prior **judicial or independent review** is indispensable before authorities can access such metadata.
8. While the case was about **access** to metadata, the Court stressed that access to **retained traffic/location data** has a **serious impact**, and “Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation that permits public authorities to have access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, **without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security, and that is so regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period.**” (para. 45).
9. In *G.D. v Commissioner of An Garda Síochána* (5 April 2022, C-140/20), the Court restated that **traffic and location metadata** are highly revealing and their indiscriminate retention is disproportionate. By contrast, **civil identity data** are treated differently: retention of subscriber name/address is allowed because they do not, in themselves, permit precise conclusions about private life. The Court thus operationalised a **distinction** whereby access to traffic or location data

results in severe interference with fundamental rights while accessing identity/IP data is less intrusive, thus the latter case would permit retention with appropriate safeguards.

10. In *Bundesrepublik Deutschland v SpaceNet & Telekom Deutschland* (20 September 2022, C-793/19, C-794/19), the Court confirmed that general and indiscriminate retention of traffic and location data is precluded, subject only to the exceptional case of legislative measures justified by a serious threat to national security, while distinguishing this from the permissible general retention of other types of data, such as IP addresses and civil identity data, under strict conditions. There is therefore no preclusion for legislative measures that, for the purposes of combating serious crime and preventing serious threats to public security, provide for:
  - the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;
  - the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;
  - the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and
  - recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,
  - provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.
11. In *A.G.* (7 September 2023, C-162/22), the Court clarified that data retained under ePrivacy for criminal purposes cannot be repurposed for other proceedings (e.g., administrative misconduct). The Court states that once the traffic and location data “have been retained and made available to the competent authorities for the purpose of combating serious crime, such data cannot be transmitted to other authorities and used in order to achieve objectives, such as, in the present case, combating corruption-related misconduct in office, which are of lesser importance in the hierarchy of objectives of public interest than the objective of combating serious crime and preventing serious threats to public security.” (para. 41)
12. In *La Quadrature du Net (II) – HADOPI* (30 April 2024, C-470/21), the Court sharpened the distinction between different types of metadata: **IP addresses** can be retained generally to combat offences in general, *but only* if safeguards guarantee that they **cannot be linked** at the retention stage with **metadata (traffic/location data)**. The reasoning hinges on the idea that **metadata are uniquely sensitive**, because once combined with identity/IP data, they allow profiling of private life.
13. The Court thus elevated “**non-linkability**” at the retention stage into a key principle: metadata must remain logically/technically separate from other identifiers unless strict safeguards and proportionality are met, stating that “a Member State which seeks to impose on providers of electronic communications services an obligation to retain IP addresses, in a general and indiscriminate manner, in order to achieve an objective linked to combating criminal offences in

general must ensure that the arrangements for the retention of those data are such as to ensure that any combination of those IP addresses with other data, retained in compliance with Directive 2002/58, which would allow precise conclusions to be drawn about the private life of the persons whose data are thus retained, is ruled out.” (para. 83)

14. In *Procura della Repubblica di Bolzano* (30 April 2024, C-178/22), the Court clarified that Article 15(1) of Directive 2002/58/EC, read in light of Articles 7, 8, 11 and 52(1) of the Charter, does not preclude national legislation allowing judicially-authorized access to retained traffic or location data for investigating offences punishable by a maximum sentence of at least three years’ imprisonment, provided that access is based on sufficient evidence, is relevant for establishing the facts, and is subject to effective prior review by a court with discretion to refuse if the offence is manifestly not serious. The Court thus reaffirmed that such access constitutes a serious interference with fundamental rights and is permissible only where it respects the principles of proportionality, necessity, and strict judicial oversight.

### **Considerations on the legal basis of the proposed instrument**

1. According to the principle of conferral, the EU may legislate only if competence has been granted by the Treaties. The central question is whether a legal basis exists for Union acts on data retention, and if so, which provisions apply.
2. Initially, Data Retention Directive 2006/24/EC relied on Article 114(1) TFEU (internal market competence). The European Court of Justice confirmed this legal basis, reasoning that the Directive regulated obligations for telecommunications companies rather than law enforcement activities. However, the Court later annulled the Directive in its judgement *Digital Rights Ireland* (joined cases C-293/12 and C-594/12) due to disproportionate interference with privacy rights. To comply with proportionality, new legislation would need to restrict law enforcement access to serious crime cases. At first sight, such rules would fall outside Article 114 TFEU, as they concern public security and criminal law and therefore fall within the competence of the member states. This creates a legal dilemma: proportionality requires rules on access, but these appear to lie beyond the scope of Article 114.
3. Yet, a closer look reveals that this dilemma may not be as strict as sometimes suggested. While Article 114 cannot serve as a basis for regulating the activities of national law enforcement authorities — that would indeed require Article 87 TFEU — the obligations of electronic communications service providers can be shaped under Article 114. In other words, the EU legislator may not be able to prescribe to Member States *who* may access data and *under what substantive conditions*, but it may limit the disclosure obligations imposed on service providers, thereby indirectly circumscribing the scope of access.
4. Support for this interpretation can be drawn from the CJEU’s case law on Article 15(1) of the ePrivacy Directive 2002/58, which itself is based on internal market competence. In *Tele2 Sverige AB* (C-203/15, paras. 72 et seq.), the Court clarified that EU law may set boundaries for the retention and disclosure duties of providers without thereby directly regulating the activities of public authorities. Similarly, the former Data Retention Directive already included an Article 4, which did not specify which authorities would have access or the detailed conditions of such access, but clarified that access must always be limited and in accordance with necessity, proportionality, and EU fundamental rights standards. Such clarifications can be justified as internal market measures, ensuring uniform obligations for providers while respecting fundamental rights.

5. An alternative legal basis lies in Article 87(2)(a) TFEU, under the Title “Area of Freedom, Security and Justice.” This provision allows measures on the collection, storage, and exchange of information for police cooperation. However, it only covers cross-border cooperation, not purely domestic law enforcement, reflecting Member States’ limited delegation of sovereignty in criminal matters.
6. In conclusion, a Union act based solely on Article 114 TFEU may regulate data retention obligations for companies and may also, in line with proportionality, include clarifications that retained data cannot be subject to unrestricted access. Provisions going further, especially those directly concerning the powers of law enforcement authorities, require Article 87(2)(a) TFEU and are limited to cross-border cooperation. Thus, EU competence in this area remains fragmented and legally constrained, but the scope of Article 114 TFEU should not be interpreted too narrowly: it can sustain rules that indirectly restrict access by defining the obligations and limitations incumbent on service providers.

## Recommendations

1. The CCBE has already elaborated in detail on the principles that must be reflected in any law that regulates access to citizens’ data, including lawyers.<sup>3</sup> The CCBE would like to recall some of them here and add several considerations which it feels are necessary to be examined further in the impact assessment that is to accompany the proposed legislative instrument.
2. First and foremost, the CCBE recommends that there be **explicit provisions protecting professional secrecy/legal professional privilege** and that the proposed legislative instrument introduces a **minimum standard of such protection**. With a view to the extremely sensitive nature of these fundamental rights which are inseparable with the national safeguards for the rule of law, a maximum harmonisation approach should be excluded in this area. Secondly, the CCBE recommends that the proposed instrument include various provisions that give effect to such protection and that ensure **respect for fundamental rights, especially the right to a fair trial and the right to defence**.
3. To this end, there should be **clear and precise definitions** as to, among other things, the types of data to be retained by the providers and the situations in which access to data is exercised by the law enforcement authorities. In particular, the concepts of national security, serious crime, extremism, terrorism, or crisis as justificatory elements in relation to the access and processing of communications should be defined with adequate specificity and clarity.
4. Any access to personal data by law enforcement authorities must be subject to **prior authorisation** provided by a Court. The judge giving approval to a request for collection should not be the same as, where applicable, the judge supervising the implementation of any access for which permission may have been given. Under no circumstances the judge who has given approval can be a judge in a later criminal procedure based on the acquired data. In those jurisdictions which envisage a role for the president of the Bar or other Bar authority, for example being present during searches or notified about the planned access to data, the special rules governing the granting or execution of the warrant should continue to be respected. Such provisions exist in Belgium, France, Italy and Slovenia.

---

<sup>3</sup> See: [‘CCBE Recommendations on the protection of client confidentiality within the context of surveillance activities’](#) and [‘CCBE Recommendations on the protection of fundamental rights in the context of “national security”’](#)

5. Consequently, there should be **specific provisions regulating the obligatory identification and handling of information that is or may be protected by professional secrecy and legal professional privilege** during the investigation so as to eliminate the risk that it may subsequently be used. This usage concerns both the introduction as evidence into proceedings, but also indirect use to obtain lawful evidence as an illegal infringement of fundamental rights should not be rewarded. Law enforcement authorities should also be required to use all means available to leave such information out of the scope of access requests. Such procedures should also exist on the side of the service providers (*infra*, nr. 11).
6. In cases where lawyers themselves are suspected of having committed a crime, and a warrant is granted to access lawyer-client communications, there needs to be supervision at all stages of the investigation, on a case-by-case basis, and the possibility for involvement of his/her professional association. This is to guarantee the PS/LPP protection of all of the lawyers' clients whose affairs are irrelevant to the investigation in question.
7. Regarding the specific protections to PS/LPP available in legislation, the ECtHR in *Denysyuk and others v Ukraine* (Applications nos. 22790/19 and 3 others) criticized that the procedures regulating covert investigatory measures contained no specific guidelines detailing the content of the legal provisions concerning the protection of lawyer-client communications. It also observed that it was not apparent that there existed any other publicly available instruments in domestic law which set out specific safeguards to be applied and procedures to be followed in cases where the authorities accidentally intercept a suspect's privileged conversation with his or her counsel in the course of telephone tapping, audio monitoring or other similar operation. The Court commented that it was therefore not clear how privileged communication should be identified, processed and destroyed, in order to fulfil the requirements of domestic law. The Court also observed that the judicial authorities, who authorised the covert investigative measures, had no competence to supervise the implementation of their rulings, and that their powers are limited to the initial authorisation stage and that there were no other authorities sufficiently independent from those involved in the case for the purposes of prosecuting the purported offence.<sup>4</sup> The Court's conclusion was that there was a violation of Article 8.
8. In this context, **the CCBE recommends that there be further examination of the impact of the proposed measure on the procedures and handling of communications covered by professional secrecy/legal professional privilege given the varying protections at national level.**
9. Legislation should not prevent lawyers from adequately protecting the confidentiality of their communications with clients (through e.g. using services that do not require storing metadata) and should not give state agencies or law enforcement authorities privileged access to such data, whether encrypted or not.
10. Legislation must also include the possibility for the providers to refuse handing over the requested data to law enforcement authorities on the grounds that it is covered by professional secrecy/legal professional privilege.
11. Any information accessed in application of EU legal instruments but without (prior) judicial authorisation and in violation of the principle of professional secrecy or legal professional privilege should, in application of a specific legal provision to that extent, be ruled inadmissible in a court of law in order to guarantee the effectiveness of the safeguards that should be included. The CJEU ruled in *Encrochat* that: "in the absence of EU rules on the matter, it is for the national legal order of each Member State to establish, in accordance with the principle of procedural autonomy,

---

<sup>4</sup> [DENYSYUK AND OTHERS v. UKRAINE](#), (Applications nos. 22790/19 and 3 others – see appended list), 13 February 2025 (paragraphs 111 and 112)

procedural rules for actions intended to safeguard the rights that individuals derive from EU law, provided, however, that those rules are no less favourable than the rules governing similar domestic actions (the principle of equivalence) and do not render impossible in practice or excessively difficult the exercise of rights conferred by EU law (the principle of effectiveness) (see, to that effect, judgments of 16 December 1976, *Rewe-Zentralfinanz and Rewe-Zentral*, [33/76](#), [EU:C:1976:188](#), paragraph 5, and of 6 October 2020, *La Quadrature du Net and Others*, [C-511/18](#), [C-512/18](#) and [C-520/18](#), [EU:C:2020:791](#), paragraph 223)." (M.N., 30 April 2024, C-670/22, para 129).

12. However, simply providing for evidence exclusion rules in the case in which unauthorised use is made by law enforcement authorities of metadata regarding communications between lawyers and clients, is not a panacea.
13. Even when metadata are not formally used as evidence against a suspect, they can still be used by law enforcement and prosecuting authorities to further shape their evidence gathering.
14. In some legal systems, this is even explicitly permitted, by using such data as "intelligence," without disclosing their origin. For instance, Belgian law allows for such use of intelligence that "permits the investigation to be directed in a certain way and subsequently to gather evidence independently":
  - to be taken into account, without specifying how the intelligence was obtained, as long as it is shown that this did not occur unlawfully (Cass. 10 September 2013, AR P.13.0376.N, Arr. Cass. 2013, no. 434); and
  - in principle, even to be used if it is established or made plausible that the intelligence was obtained unlawfully, unless it is demonstrated in concreto that its use constitutes a violation of Article 6 ECHR (Cass. 27 June 2017, AR P.15.0814.N, Arr. Cass. 2017, no. 423).
15. Such national case law and the possibility of making informal use of illegally collected metadata regarding communication between lawyers and their clients to steer a criminal investigation clearly also poses a threat to the practical and effective protection of the aforementioned guarantees.
16. This clearly shows that it is not only necessary to prevent such protected metadata from being *used as evidence* by law enforcement and prosecuting authorities, but also from being *shared* with them. That responsibility should be borne both by law enforcement authorities and by service providers who hold the metadata in question.
17. Any lawfully accessed material should be used solely for the purpose for which the authorisation of the oversight body was granted, exceptions should be clearly identified by law in accordance with fundamental rights.
18. In order to provide effective legal protection against unlawful surveillance, it is necessary that legal remedies are made available to lawyers and their clients who have been the subject of unlawful surveillance; further, where appropriate, sanctions should be imposed upon those persons and agencies who have undertaken such unlawful surveillance.
19. In particular, once it has been disclosed that surveillance measures have been undertaken, lawyers and their clients must have the right to be informed of the data collected as a result of direct or indirect surveillance. Such provisions already exist in Article 13 of the Data Protection Law Enforcement Directive (EU) 2016/680 or Article 13 of the e-Evidence Regulation (the latter relying on the relevant provisions of the LED). The CCBE notes that the first evaluation of the LED observed that: '*Individuals are also increasingly using their right to lodge complaints with data protection*

*supervisory authorities, including in cases where competent authorities limit the exercise of data subjects' rights. More than a third of data protection supervisory authorities reported an increase in the number of complaints received following the transposition of the LED in their Member States. Some of the most frequent complaints received by data protection supervisory authorities concerned the limitation to the right of access, the right to rectification or erasure, and the right to information and the limitations thereto. These were followed by complaints related to the storage limitation principle, which requires competent authorities to keep personal data for no longer than necessary, and to the right to information.*<sup>5</sup> Furthermore, the Court of Justice of the EU (CJEU), in *CG v Bezirkshauptmannschaft Landeck*, stressed the importance of the right to be informed as a fundamental pillar of the right to an effective remedy. The CCBE would recommend that the impact assessment include more in-depth considerations of how the right to information can be exercised in the context of the proposed legislative instrument. This is all the more important in the case of cross-border instruments for recovery of evidence which add one more layer of complexity in the defence's efforts to scrutinise foreign evidence.

20. Furthermore, these are important provisions given that the entire defence is built based on the evidence and the capability to assess its legality and admissibility. This is why an early access to case file and in this case, information about data being accessed and for what purpose, is crucial to examine the evidence and provide effective defence. This is why the principles of notification and information to the persons concerned are crucial – they allow for time to prepare defence.
21. Once it has been disclosed that one's data had been accessed, lawyers and clients who have been affected should be able to challenge the legality of such measures before a court. Similarly to what the CCBE has advocated in the context of the e-Evidence Regulation<sup>6</sup>, persons affected by an order to access data should be able to exercise their remedies before the court of the country of their residence. Therefore, the CCBE recommends that the impact assessment look more into detail of how effective remedies can be ensured in the proposed instrument.
22. All law enforcement authorities which have been found to have accessed data illegally should be made liable and have sanctions imposed upon them.
23. The CCBE recommends that the impact assessment look more in depth into the question of presumption of innocence and how the proposed instrument will impact this important right. There are instances where accessing data on the basis of geographical location or on the basis of the criminal history may have an impact on the affected communities. Also, in a digitalised world more contacts of any kind leave a trace of (meta)data. The impact assessment should assess how wrong suspicions and a criminalisation of innocent citizens can sustainably be prevented.
24. The CCBE also recommends that the proposed instrument has provisions setting out clear and foreseeable conditions for issuing production orders/warrants, such as proper justification, reasonable suspicion and judicial oversight. To this end, the concepts of national security, extremism, terrorism, or crisis as justificatory elements in relation to the processing of personal data should be laid down with adequate specificity and clarity. The requests for data should be specific in terms of the addressees/subjects/types of data requested/clear indication of the time period for which the data are requested.

---

<sup>5</sup> [First report on application and functioning of the Data Protection Law Enforcement Directive \(EU\) 2016/680](#) ('LED'), Brussels, 25.7.2022, COM(2022) 364 final, page 17

<sup>6</sup> See: [CCBE position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters](#) (2018)