A Plea for Common Standards on the Lawyer-Client Privilege in EU Cross-Border Criminal Proceedings in Light of Advancing Digitalisation

Lorena Bachmaier *

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

ABSTRACT

While the right to lawyer-client confidentiality has long been recognised as a fundamental right enshrined in the right to legal assistance and the right of defence, its practical implementation does not seem to provide adequate safeguards. Many EU Member States still lack clear rules on how to ensure that privileged communications are not captured during the interception of communications and the search/seizure of computers during criminal investigations. Also, OLAF investigations struggle with deficiencies in safeguarding the lawyer-client privilege. Taking the case law of the European Court of Human Rights as a starting point to identify common standards on the lawyer-client privilege in criminal proceedings, this article argues that there is a need for the European Union to take legislative action to ensure the effective protection of this right.

AUTHOR

Lorena Bachmaier

Full Professor of Law
Universidad Complutense Madrid

CITATION SUGGESTION

L. Bachmaier, "A Plea for Common Standards on the Lawyer-Client Privilege in EU Cross-Border Criminal Proceedings in Light of Advancing Digitalisation", 2024, Vol. 19(3), eucrim, pp222–229. DOI: https://doi.org/10.30709/eucrim-2024-016

Published in
2024, Vol. 19(3) eucrim pp 222 – 229
ISSN: 1862-6947
https://eucrim.eu

CC BY ND

I. Introduction

The Charter of Fundamental Rights of the European Union (CFR) and the European Convention on Human Rights (hereinafter: ECHR or the Convention) do not expressly guarantee the defendant's right to communicate confidentially with his/her defence attorney. However, this right is enshrined in the fair trial safeguards of Arts. 47 and 48 CFR and in Art. 6 ECHR. The ECtHR has been very attentive when it comes to protecting this right, and the content and scope of the right to lawyer-client confidentiality has been continuously clarified in its case law. The Court of Justice of the European Union (CJEU) has addressed the lawyer-client privilege and legal professional secrecy only in few judgments so far,[1] which is why ECtHR case law is paramount for defining EU common standards on this matter.

The Strasbourg Court has repeatedly declared that the lawyer-client privilege and the confidentiality of their communications is the basis of the relationship of trust that must exist between the lawyer and his/her client. It has also stressed that this privilege is one of the core elements of the right to a fair trial in a democratic society.[2] This right is set out in Art. 6(3) lit. c) ECHR and covers face-to-face/oral communications, as well as communications by post or by telephone, or by way of any electronic system. In addition, the ECtHR stressed that the safeguarding of professional secrecy is the corollary of the right to legal assistance and the right against self-incrimination.[3] Any interception of the communications between lawyer and client in criminal proceedings falls within the scope of private life and implies an interference with Art. 8 ECHR, which can also entail an infringement of Art. 6 ECHR.[4] The protection of the confidentiality of these privileged communications has become even more challenging in the digital environment, in which law enforcement access to electronic data and communications is likely to be done without filtering these communications.

While certain common standards have been set out by the ECtHR, there are still important differences in the protection of the right to lawyer-client confidentiality at the national level.[5] Such asymmetries within the EU entail important risks in transnational criminal proceedings and may lead to violations of this right in the context of cross-border evidence gathering. Taking the example of investigations into offences detrimental to the EU's financial interests, it can be seen that there is further a lack of precise provisions for the digital investigative operations carried out by OLAF, despite the high standards on digital forensics.[6] Against this background, this article makes a plea for the protection of the lawyer-client privilege at the European Union level. It explores specific safeguards for the access of data that might contain privileged communications.

To advance towards an EU legislative framework, it is important to first take stock of the content of the right to the lawyer-client privilege as defined by the ECtHR in its case law.[7] I will summarise the ECtHR's case law on certain investigative measures, precisely on access to and interception of communications of lawyers; entry and search of lawyers' offices and computers; and access to electronic data, since these are measures that entail a high risk of violating the lawyer-client privilege.[8] After reviewing the standards defined by the Strasbourg Court, I will point out some of the problems that might emerge in cross-border criminal proceedings in the area of freedom, security and justice, not only as regards the protection of the lawyer-client privilege in OLAF's digital investigations, but also when executing a European Investigation Order (EIO) and within the context of the future application of the Regulation on the European Production and Preservation Orders for electronic evidence. Lastly, I will argue in my conclusions that European Union law should comprehensively address the protection of the right to lawyer-client confidentiality in transnational criminal proceedings to effectively ensure the right of defence and also to prevent problems regarding the admissibility of cross-border criminal evidence.

II. Overview of the ECtHR Case Law on the Lawyer-Client Privilege in Criminal Investigations

The protection of the lawyer-client privilege is recognised in several recommendations of the Council of Europe's Committee of Ministers and Parliamentary Assembly.[9] In addition, the United Nations adopted in 1990 the *Basic Principles on the Role of Lawyers*.[10] The ECtHR developed several principles on the lawyer-client privilege, which can be summarised as follows:

- Any person who wishes to consult a lawyer should be free to do so under conditions which favour full and uninhibited discussion;[11]
- The protection of confidentiality is not limited to the protection of communications or actions related to pending proceedings;[12]
- The right to confidentiality of lawyer-client communications must be guaranteed in such a way that its exercise is effective and not merely formal.[13]

The ECtHR differentiates between interferences in conjunction with the right of Art. 8 ECHR (right to respect for private life and correspondence) because of measures adopted in the context of a criminal investigation, on the one hand, and the impact that the violation of the right to the lawyer-client confidentiality may have on the rights guaranteed under Art. 6 ECHR, on the other.[14] The seizure of a client's documents that are in the possession of his/her lawyer and that are obtained without respecting the right to professional secrecy, can also constitute a violation of the right against self-incrimination.[15]

Since *Golder v. United Kingdom*[16] and *Niemietz v. Germany*,[17] the Court has been defining the requirements that must be met so that interference in the lawyer-client privilege can be considered to be in accordance with the Convention.[18] These requirements are analysed when addressing the different investigative measures.

1. Interception of telephone communications

The right to defense and legal assistance would not be effective without the protection of the confidentiality of lawyer-client communications. Although not all conversations between the lawyer and his/her client are protected by the lawyer-client privilege, all European legal systems strictly prohibit intercepting the telephone of a lawyer who is not suspected or charged with a criminal offence, because Art. 8 ECHR protects the confidentiality of any "communication" and in addition grants a reinforced protection to communications between lawyers and their clients.[19] In practice, the major problem arises from communications that are accidentally intercepted when the defendant's telephone is tapped or his/her computer searched. [20] Indeed, there is consensus that it is almost impossible to prevent some of these conversations from being overheard or even recorded, and the ECtHR has put the focus on the need for a legal regulation providing for adequate safeguards, such as the destruction of the recordings.[21] However, the Court has not gone so far as to impose an exclusionary rule of evidence on the states.[22]

2. Entry, search and seizure: Specific requirements for seizing computer files of lawyers and in law offices

Most legal systems only authorise the entry and search of a law firm and its files and computers, when the lawyer himself/herself is the suspect of a crime,[23] but there are still many countries that will allow this measure even if the lawyer is not the suspect. The ECtHR takes a much stricter approach if the search is

carried out in the office of a lawyer who is not a suspect,[24] requiring "compelling reasons" to justify such interference in Art. 6 and eventually Art. 8 ECHR.[25] The ECtHR has accepted such measures if there is an adequate and sufficient legal provision, namely if the objective pursued is legitimate and meets the requirement of necessity and proportionality, and the search can be carried out respecting the adequate safeguards.[26]

a) Safeguards developed by the ECtHR

In the case law of the Court, most judgments that have found a violation of Art. 8 ECHR were based on the lack of a sufficient legal provision and, specifically, because the legal framework did not provide for specific safeguards to protect lawyer-client confidentiality.[27] According to the Court,[28] the national law must specify who shall execute the measure and how the search and seizure shall be carried out, including detailed rules on how electronic data related to the crime under investigation should be accessed and what safeguards are in place to avoid abusive searches and the seizing of privileged files. If such legal safeguards are in place, the Court proceeds to check whether they have been effectively implemented during the search and seizure of the lawyer's office. The ECtHR, in particular, has paid special attention to the following two circumstances:

1. **Whether the judicial warrant is issued upon reasonable suspicion and whether the scope of the search and seizure is limited**

This is not a mere formality;[29] in order to comply with the Convention, the scope of the search and seizure must be clearly limited, especially when it comes to computer searches and access to electronic files in order to ensure the principle of proportionality.[30] The ECtHR noted that, where a court order allows the search and seizure of all personal computers and data storage devices without limiting the search to those files likely to contain evidence and be relevant to the ongoing criminal investigation, such broad authorisation is not compatible with the guarantees that must be respected in order to protect professional secrecy, therefore constituting a violation of Art. 8 ECHR.[31]

1. **Whether sufficient safeguards were adopted to protect professional secrecy during the search and seizure**

Some of the safeguards the ECtHR has taken into account when assessing possible violations of the Convention, include the following:[32]

- A procedure for separating privileged documents/material, so that they are not seized;
- Measures to prevent officers from accessing the privileged documents/material;
- The search is carried out in the presence of the lawyer and he/she has the chance to identify any documents/material protected by the right to confidentiality and to ensure that the number of seized elements is not disproportionate;
- The presence of an independent observer who can monitor that files protected by professional secrecy are not seized.
- In some cases, as a reinforced safeguard, the presence of a judge during the search, who supervises that it complies with the court order.[33]

The ECtHR considers the presence of an independent third party with sufficient qualifications to ensure that documents/material protected by professional secrecy are not seized an important safeguard for the conformity of the entry and search of a law firm, in line with the Convention and therefore an almost absolute requirement.[34] However, the presence of the lawyer and two witnesses was not considered sufficient in a number of cases.[35]

As to the safeguards that need to be in place in order to protect files and communications subject to the lawyer-client privilege, the Court has laid down guidelines regarding the search and seizure of computers and electronic files.[36]

b) Problems in practice and the ECtHR's reaction

The investigative measures of search and seizure of computers and electronic files continue to pose problems in practice, since most legal systems do not include detailed rules on how the measures should be executed. The judicial warrant authorising the search and seizure often only specifies the type of documents that can be sought and seized but not the keywords or search programmes to be used to identify the files protected by the lawyer-client privilege. The case of *Wolland v. Norway*[37] is interesting in this respect, as it shows the detailed procedure to be followed according to Norwegian law in cases of computer searches as well as all the safeguards provided to prevent privileged documents and communications from being accessed and seized.[38]

Furthermore, although on-site searches should be the rule, this is not always feasible, and it is common practice for police officers to seize all the hardware and computers and move them to designated premises in order to carry out the examination by public IT officers or independent computer experts in a forensic laboratory.

In the case of *Särgava v. Estonia,* which dealt with the search of electronic devices of lawyers, the ECtHR made a very clear statement on the need to separate the files protected by the lawyer-client privilege and that this safeguard is of utmost importance when it comes to electronic data and searches of electronic devices:[39]

> While the question of sifting and separating privileged and non-privileged files is undoubtedly important in the context of hard copy material, it becomes even more relevant in a situation where the privileged content is part of larger batches of digitally stored data. In such a situation, even if the lawyer concerned or his representative is present at the search site, it might prove difficult to distinguish swiftly during the search which exact electronic files are covered by legal professional privilege and which are not.

The question of how to carry out sufficiently targeted sifting is equally pertinent in circumstances where under domestic law or practice such sifting is not carried out at the site of the search, but the data carriers are instead seized in their entirety and/or a mirror-image copy of their content is made. The Court has acknowledged that cloning the devices might be necessary to prevent illicit data tampering with the device. It has also allowed the devices to be quickly returned to their owner(s) but required measures to be adopted to guarantee that, during the copying and screening of the content of the devices, data not covered by the judicial authorisation and privileged data are not accessed or seized.[40]

In *Särgava v. Estonia,* the Court found a violation of the Convention, taking into account the following:[41] the judicial order did not specify the measures to be adopted in order to protect professional secrecy, even though it was already known that protected documents were stored on the seized devices; the national law neither established the procedure to be followed to access electronic data nor did it contemplate specific measures guaranteeing that the protection of professional secrecy would be guaranteed during the examination of the devices; the person under investigation neither participated in nor was present during the selection of the search terms and files to be examined in the criminal proceeding. This case is highly relevant, because, according to the ECtHR, the absence of a legal regulation with specific provisions on the handling of electronic files and the sifting through of privileged documents already constitutes a violation of

Art. 8 ECHR, even if, in practice, the measure was executed respecting the principle of proportionality after a sound perusal of the files.

In conclusion, for the Court, the absence of a clear procedural scheme that defines how the search of electronic devices must be carried out with full guarantees, and the fact that the law does not establish safeguards to prevent the privileged documents from being downloaded and read by investigators once the computers have been seized, entails a breach of the Convention.[42]

III. Lawyer-Client Privilege and the Cross-Border Gathering of Evidence in the EU

Looking first at the lawyer-client privilege in investigations related to the protection of the EU's financial interests, there is a complete set of guidelines to be followed in digital forensic procedures carried out by OLAF: Guidelines on Digital Forensic Procedures for OLAF Staff.[43] These guidelines not only provide for technical standards but also for legal standards to ensure defence rights and also compliance with the principle of proportionality. With regard to the protection of privileged material, the guidelines set out that if, during an "on-the-spot check" operation, the representative of the economic operator claims that the device being inspected contains legally privileged data, such data is to be acquired and placed in a sealed envelope.[44] Furthermore, the guidelines provide that, before opening the envelope, the economic operator "will be invited for a meeting to resolve the issue". To this end, he/she may be assisted by a person of his/her choice.

This safeguard is adequate to prevent the lawyer-client privilege – and other privileged materials – from being infringed during the collection of digital evidence; providing for the entity's representative to be present while the data are analysed and/or sifted is also a positive measure. However, such provisions are not sufficient to effectively protect the lawyer-client privilege, since the guidelines do not establish how the sifting is to be done. To prevent disclosure and access to privileged data, more detailed provisions would need to be adopted in order to ensure that the OLAF investigation report is not excluded as evidence in a subsequent criminal procedure.

Looking second at accessing cross-border evidence within the EU, the following paragraphs will deal with two EU instruments: the Directive on the European Investigation Order (hereinafter DEIO)[45] and the Regulation on European Production and Preservation Orders for electronic evidence (hereinafter EPO/EPRO-Regulation).[46]

1. The European Investigation Order

The DEIO is based on the principle of mutual recognition, nonetheless providing a quite extensive list of refusal grounds (mainly, but not exclusively, stipulated in Art. 11). This scheme introduces some flexibility in the execution of an EIO and avoids "blind" recognition, which might be contrary to procedural principles and safeguards. Among the refusal grounds, Art. 11(1) DEIO lists the existence of an immunity or a privilege under the law of the executing state.[47]

Very frequently, the breach of the lawyer-client privilege occurs by way of accidental interceptions of the communications or documents of the suspect or a third person, thus cases in which the lawyer or his/her offices and electronic devices are not the target. In practice, these interferences into the right to lawyer-client confidentiality are almost impossible to avoid and hence the protection of this right needs to be done *ex post*, by preventing such material from reaching the trial and/or being used as evidence. As a rule, the grounds for refusal for executing the EIO would not play a role here, because the accidental interception of privileged communications can neither be foreseen nor avoided beforehand.

Other means of access to privileged files and communications of a lawyer in execution of an EIO can be: during the entry and search of the lawyer's office; and accessing the lawyers' computers or other digital devices (remotely or located outside the office). In principle, such measures are not to be refused if they are provided for in the executing state for similar cases.

However, the most problematic question relates to the way in which the search and seizure of documents/data should be carried out, so that the executing state respects its own procedural rules on protection of privileged material and, at the same time, complies with the *lex fori* to ensure that the evidence gathered will be admissible as evidence. There is no legal harmonisation on how to proceed with regard to the safeguards for filtering privileged and non-privileged files/communications.

Furthermore, the exclusionary rules of evidence among the EU Member States also differ from each other, and thus the effective protection of the lawyer-client privilege might become completely ineffective if, for example, the seized electronic files are not filtered in the executing state and the privileged communications are not excluded as evidence in the forum state. The problems deriving from the absence of common rules on the admissibility of evidence in criminal proceedings have been pointed out numerous times:[48] as long as the evidentiary rules are not adequately harmonised among the different Member States, the transfer of evidence from one country to another will impact the level of procedural safeguards and the rights of the defence.[49] The issue that arises here is how to protect the fundamental right to the confidentiality of lawyer-client communications when executing an EIO? Which system of sifting the data should be in place? Who should control it? Should the filtering of data be carried out *in situ*? If so, according to which rules? What happens when the EIO defines the scope of the search and the type of data to be seized but does not specify the keywords to be used or the way in which the data should be sifted to prevent unlawful interference into the right to lawyer-client confidentiality?

Problems arise if the executing authority has adopted its own protocols for separating the privileged materials, but these are not provided in a legal provision and thus might not be in accordance with ECtHR case law. Would the evidence obtained in such a way, lacking a sufficient legal basis in the executing state and thus being in breach of the ECHR, be admissible as evidence in the forum state? The general rule is that, if the *lex loci* has been complied with, the evidence should be admissible unless the evidence has been obtained in violation of human rights. And, according to the ECtHR, if safeguards to prevent interference with the lawyer-client privilege were not sufficiently regulated in the (national) law, the ECHR has not been complied with.

If the issuing state requires the executing state to exclude privileged information, but the issuing authority nevertheless receives privileged data, how should this situation be dealt with? Should the receiving authority simply exclude them and carry out the sifting in the issuing state, or would this circumstance already lead to a violation of the lawyer-client privilege?

Indeed, when the files seized include materials or communications covered by the lawyer-client privilege, it would mean that the safeguards to prevent such a violation were not adequate or not adequately implemented when carrying out the search and seizure. The lack of safeguards or non-compliance with them would amount to a breach of the Convention according to the ECtHR case law described above.

Lastly, the issuing authority might request the complete cloning of a computer in the executing state and the sending over of the complete data to be filtered according to the laws of the forum. The ECtHR has admitted that the quantity of the files searched and seized is not *per se* contrary to the Convention if there are adequate counterbalancing safeguards in place to protect the right to lawyer-client confidentiality. In this case, what would be the counterbalancing measures to be checked?

2. European Production Order for e-evidence

With regard to the rules for protecting the lawyer-client privilege in the context of access to electronic data by way of a European Production Order (EPO),[50] the relevant safeguards are provided in Art. 5 EPO/EPRO-Regulation. The Regulation implies the following principle:[51]

> [I]t should be possible for the enforcing authority, where it is notified pursuant to this Regulation, to refuse a European Production Order where the data requested are protected by immunities or privileges granted under the law of the enforcing State which prevent the execution or enforcement of the European Production Order […].

As regards the safeguards for privileged data, the Regulation distinguishes between two situations. The first situation is found in Art. 5(9) EPO/EPRO-Regulation, which reads as follows:

> In cases where data protected by professional privilege under the law of the issuing State are stored or otherwise processed by a service provider as part of an infrastructure provided to professionals covered by professional privilege ('privileged professional'), in their business capacity, a European Production Order to obtain traffic data, except for data requested for the sole purpose of identifying the user as defined in Art. 3, point (10), or to obtain content data may only be issued:
>
> (a) where the privileged professional resides in the issuing State;
>
> (b) where addressing the privileged professional might be detrimental to the investigation; or
>
> (c) where the privileges were waived in accordance with the applicable law.

This provision seeks to protect the professional privilege, first by way of preventing the issuing of an EPO to obtain traffic (save for identification of the user) and content data of a lawyer, requiring the issuing authority to check (1) whether the lawyer resides in the forum state; or (2) whether the data cannot be obtained directly from him/her (because this would be detrimental to the investigation); or (3) whether the privilege has been waived. In any event, once the EPO has been issued to request traffic or content data, the authority (judge) of the enforcing state who is to be notified (Art. 8 EPO/EPRO-Regulation) will also have to check whether these conditions are met.

The second paragraph of Art. 5(10) EPO/EPRO-Regulation establishes that, if the issuing authority has "reasons to believe" that the traffic or content data requested are protected by professional privilege under the laws of the enforcing state, it shall not issue the EPO –and, if issued, in accordance with Art. 12 (1) (a) the authority in the enforcing state can invoke a ground for refusal.

This provision prevents Internet Service Providers (ISPs) as addressees from enforcing the EPO if the requested traffic or content data are protected by the lawyer-client privilege in the enforcing state. Of course, an ISP is not expected to check this, since it would be almost impossible to do so. Therefore, the Regulation relies on the proper examination by the issuing authority when sending out such an EPO, namely that it has "reasons to believe" that such data are covered by legal privilege.

In contrast to the EIO, Art. 5 (9) and (10) of the EPO/EPRO-Regulation is not based on mutual recognition but on prohibiting cross-border cooperation to access traffic or content data that are privileged under the *lex loci*. This mechanism is clearly more restrictive than the applicable rules under the EIO – where the privilege might be invoked as a ground for refusal: the Regulation states that privileged data are not subject to being accessed by an issuing authority by way of an EPO if they are also protected in the enforcing state. Since the

lawyer-client privilege is protected in all EU states, an EPO cannot be issued to obtain traffic or content data covered by the Regulation. However, if the issuing authority does not have "reasons to believe" that the data requested are privileged, and the EPO complies with requirements under Art. 5 (9) EPO/EPRO Regulation, it will be up to the notified authority in the enforcing state to check this circumstance after issuance of the EPO (Art. 8 EPO/EPRO Regulation). This is problematic, because it will be difficult for the authority in the enforcing state to notice this if the issuing state does not point out some form of possible professional privilege.

In sum, the implementation of the rules provided in the EPO/EPRO-Regulation relies completely on the assessment of the issuing state ("reasons to believe") in that the EPO affects data protected by professional privilege. As a rule, neither the ISP nor the authority in the enforcing state will be able to check whether the data requested effect a legal privilege if the issuing authority does not provide any hints in this direction. And while Art. 18 EPO/EPRO-Regulation regulates the right to an effective judicial remedy, this will only be activated *ex post*. It is doubtful whether this scheme will afford sufficient protection if the national rules do not provide for an exclusionary rule of evidence in case of breach of the lawyer-client privilege.

IV. Conclusion

While the right to lawyer-client confidentiality has long been recognised as a fundamental right enshrined in the rights to legal assistance and of defence, its practical implementation does not seem to provide adequate safeguards. As outlined in this article, OLAF investigations seek to protect this privilege, but neither its legal framework nor its guidelines include sufficient safeguards; and many EU Member States still lack clear rules on how to ensure that privileged communications are not captured during the interception of communications and the search/seizure of computers. The digitalisation of society and its communications has heightened the need to implement specific safeguards to prevent unlawful access to materials protected by professional secrecy through investigative measures that breach this protective right. As seen above, the ECtHR has called for the provision of specific rules to prevent overly intrusive access to lawyer-client privileged files and communications.

Identifying the standards for protection of the fundamental right to confidentiality of the lawyer-client relationship is only the first step in future legislation on the protection of the lawyer-client privilege in criminal proceedings at the EU level – by way of a future Directive. It is not only sufficient to draw attention to the need to ensure the protection of the lawyer-client privilege; this right should also be effectively protected in the cross-border gathering of criminal evidence, especially when accessing both electronic storage devices and electronic data held by internet service providers. This article has particularly demonstrated that the rules enshrined in the Directive relating to the European Investigation Order and in the Regulation on e-evidence (EPO/EPRO-Regulation) are not sufficient to grant effective protection. It is a plea for a European legislative framework laying down common standards on the lawyer-client privilege in cross-border criminal proceedings. In my opinion, supranational legislative action is absolutely needed.

---

1. E.g., CJEU (Grand Chamber), 8 December 2022, C-694/20, *Orde van Vlaamse Balies;* CJEU, 26 September 2024, Case C-432/23, *Ordre des avocats du barreau de Luxembourg*. Both decisions deal with preliminary references related to the administrative cooperation in the field of taxation and the application of Directive 2011/16/EU.↩
2. See, for example, ECtHR, 28 November 1991, *S. v. Switzerland*, Appl. nos. 12629/87 and 13965/88, para. 48.↩
3. On the lawyer-client privilege in the USA, see the comprehensive reference book by E. Epstein, *The Attorney-Client Privilege and the Work-Product Doctrine,* ABA Publishing, Chicago, 2017.↩
4. On this issue, see generally T. Spronken and J. Fermon, "Protection of Attorney-Client Privilege in Europe", (2008) 27 *Penn State International Law Review,* 439-463.↩
5. For a broad comparative law approach, see L. Bachmaier Winter, S. Thaman, and V. Lynn, (eds.), *The Right to Counsel and the Protection of Attorney-Client Communications in Criminal Proceedings. A Comparative View*, 2020.↩

6. See the "Guidelines on Digital Forensic Procedures for OLAF Staff", 15 February 2016, accessible at: <https://anti-fraud.ec.europa.eu/document/download/87e5deb1-8a64-42ca-8e08-234355dbe544_en?filename=guidelines_en_bb84583638.pdf> accessed 11 October 2024.↩
7. On this topic, see L. Bachmaier, "Lawyer-client privilege en la jurisprudencia del Tribunal Europeo de Derechos Humanos", in: L. Bachmaier (ed.), *Investigación penal, secreto profesional del abogado, empresa y nuevas tecnologías. Retos y soluciones jurisprudenciales,* 2022, 21-79.↩
8. It would go beyond the scope of this article to address the issue of who the owner of the right to professional secrecy is and who can waive the right to the lawyer-client privilege. On this issue, see the highly debated ECtHR case *Klaus Müller v. Germany*, Appl. no. 24173/18, 19 November 2020. Analysing the problems related to execution orders in administrative taxation proceedings, which have been addressed by the CJEU, also exceeds the scope of this article. Nevertheless, it is important to underline that the CJEU has found it to be in violation of Art. 52(1) CFR if, under national law, a lawyer in tax matters does not benefit from the enhanced protection of communications between a lawyer and his client as guaranteed by Art. 7 CFR, except where there is a risk of criminal prosecution for the client (see CJEU, 26 September 2024, Case C-432/23, *op. cit.* (n. 1)).↩
9. See mainly Recommendation No. R(2000)21 *on the freedom of exercise of the profession of lawyer* (adopted by the Committee of Ministers of the Council of Europe on 25 October 2000); Parliamentary Assembly, Recommendation Rec 2085 (2016) of 28 January 2016, *Strengthening the protection and role of human rights defenders in Council of Europe Member States*; see also No. 93 of the Appendix to the *Standard Minimum Rules for the Treatment of Prisoners,* Resolution (73) 5 of the Committee of Ministers of 19.1.1973.↩
10. *Basic Principles on the Role of Lawyers* adopted on 7 September 1990, ONU Doc. A/CONF.144/28/Rev.1 p. 118 (1990), para. 22.↩
11. ECtHR, 25 March 1992, *Campbell v. United Kingdom,* Appl. no. 13590/88, para. 46. On the impact of the ECtHR's case law and the lawyer-client privilege in common law systems, see J. Auburn, *Legal Professional Privilege: Law and Theory,* 2000, pp. 37 ff.↩
12. See ECtHR, 9 April 2019, *Altay v. Turkey* (No. 2), Appl no. 11236/06, paras. 49-51.↩
13. See, for example, ECtHR, 27 April 2017, *Sommer v. Germany*, Appl. no. 73607/13, para. 56; ECtHR, 6 December 2012, *Michaud v. France*, Appl. no. 12323/11, para. 130. This requires providing specific measures and safeguards to ensure such effective protection.↩
14. See ECtHR, 21 February 1975, *Golder v. United Kingdom,* Appl. No. 4451/70, para. 45; ECtHR, 25 July 2017, *M. v. The Netherlands*, Appl. no. 2156/10, para. 85. In the latter case, the ECHR deals with the possible violation of Art. 6(3) lit. c) ECHR in a matter related to the disclosure of classified information and the restrictions on access to a lawyer and communication confidentially in the context of facts involving state secrets and national security interests.↩
15. See ECtHR, 24 July 2008, *André and Another v. France*, Appl. no. 18603/03, para. 41. However, in its assessment, the Court usually does not enter into analysing the infringement of Art. 6 ECHR once it has confirmed that there was a violation of Art. 8 ECHR.↩
16. *Op. cit.* (n. 14).↩
17. ECtHR, 16 December 1992, *Niemietz v. Germany*, Appl. no. 13710/88.↩
18. The ECtHR has also extensively addressed the right of the detainee to communicate with their lawyer as a substantial part of the right to defence and the right to legal assistance. See, e.g., ECtHR, *Golder v. United Kingdom, op. cit.* (n. 14); ECtHR, 20 June 1988, *Schönberger and Durmaz v. Switzerland,* Appl. No. 11368/85; ECtHR, 13 March 2007, *Castravet v. Moldova,* Appl. no. 23393/05; ECtHR, 4 October 2005, *Sarban v. Moldova*, Appl. no. 3456/05; ECtHR, 31 May 2011, *Khodorkovskiy v. Russia,* Appl. no. 5829/04; ECtHR, 24 May 2018, *Laurent v. France*, Appl. no. 28798/13.↩
19. ECtHR, 27 October 2015, *R.E. v. United Kingdom*, Appl. no. 62498/11, para. 131; or ECtHR, 7 November 2017, *Dudchenko v. Russia,* Appl. no. 37717/05, para. 104.↩
20. L. Bachmaier Winter, "Intervenciones telefónicas y derechos de terceros en el proceso penal", (2004) nos. 1-3 *Revista de Derecho Procesal,* 50.↩
21. This was already stated in the benchmark case ECtHR, 25 March 1998, *Kopp v. Switzerland*, Appl. no. 13/1997/797/1000. Although, in the end, the case was analysed from the perspective of insufficient legal provision, the Court highlighted the difficulty in avoiding privileged communications from being intercepted. See also ECtHR, 3 February 2015, *Pruteanu v. Romania*, Appl. no. 30181/05; ECtHR, 16 November 2021, *Vasil Vasilev v. Bulgaria,* Appl. no. 7610/15.↩
22. On the different approach towards the exclusionary rules of evidence in this context, see L. Bachmaier and S. Thaman, "A Comparative View of the Right to Counsel and the Protection of Attorney-Client Communications" in L. Bachmaier Winter, S. Thaman, and V. Lynn, (eds.), *The Right to Counsel and the Protection of Attorney-Client Communications in criminal proceedings. A Comparative View*, 2020, pp. 101 and 104.↩
23. This is the case, for example, in Portugal, Spain, and in several states of the USA, precisely Oregon and Minnesota. See L. Bachmaier and S. Thaman, *op. cit.* (n. 22), p. 55.↩
24. This was the case in ECtHR, 25 February 2003, *Roemen and Schmit v. Luxembourg,* Appl. no. 51772/99. See also ECtHR, 4 February 2020, *Kruglov and Others v. Russia*, Appl. no. 11264/04 *et al*., para. 128.↩
25. ECtHR, 25 July 2013, *Khodorkovskiy and Lebedev v. Russia*, Appl. nos.11082/06, 13772/05.↩
26. See ECtHR, 19 September 2002, *Tamosius v. United Kingdom,* Appl. no. 62002/00 (inadmissibility decision in a tax fraud case). See also ECtHR, 1 December 2015, *Brito Ferrinho Bexiga Vila-Nova v. Portugal*, Appl. no. 69436/10; ECtHR, 13 January 2009, *Sorvisto v. Finland*, Appl. no. 19348/04, para. 118; ECtHR, 15 February 2011, *Heino v. Finland*, Appl. no. 56720/09, para. 43.↩
27. See, for example, ECtHR, 27 September 2005, *Petri Sallinen and Others v. Finland*, Appl. no. 50882/99. See extensively L. Bachmaier, "Lawyer-client privilege", *op. cit.* (n. 7), 22 ff.↩
28. ECtHR, 17 December 2020, *Saber v. Norway*, Appl. no. 459/18.↩
29. See ECtHR, *Kruglov and Others v. Russia*, *op. cit.* (n. 24).↩
30. The frequent practice of cloning or mirroring the entire hard drive, both in direct computer searches and in remote computer searches, inevitably leads to the interception and seizure of documents and communications that should be excluded, because they fall under the lawyer-client privilege. See, L. Bachmaier Winter, "Remote search of computers under the new Spanish Law of 2015: proportionality principle and the protection of privacy", (2017) 129(1) *Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW)*, 1-27.↩
31. ECtHR, 3 July 2012, *Robathin v. Austria*, Appl. no. 30457/06, paras. 47, 51, 52. See also ECtHR, 22 May 2008, *Iliya Stefanov v. Bulgaria*, Appl. no. 65755/01; ECtHR, 4 October 2018, *Leotsakos v. Greece,* Appl. no. 30958/13, paras. 43, 52; 12 February 2015, ECtHR, *Yuditskaya and Others v. Russia*, Appl. no. 5678/06.↩

32. On these safeguards, see, in more detail, L. Bachmaier Winter, "Lawyer-client privilege and computer searches in law offices: the caselaw of the European Court of Human Rights and the need for common standards in transnational criminal investigations in the EU", in: M. Daniele and S. Signorato (eds.), *Volume in Onore Prof. Kostoris*, 2022, pp. 261-286, 267 ff.↩
33. See ECtHR, *Tamosius v. United Kingdom*, *op. cit.* (n. 26).↩
34. See, in particular: ECtHR, *Roemen and Smit v. Luxembourg, op. cit.* (n. 24), para. 69; ECtHR, 16 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria*, Appl. no. 74336/01; ECtHR, *André and Another v. France*, *op. cit.* (n. 15), paras. 42 and 43; ECtHR, 1 September 2009, *Jacquier v. France*, Appl. no. 45827/07; ECtHR, 21 January 2010, *Xavier Da Silveira v. France*, Appl. no.43757/05, paras. 37 and 43; ECtHR, 3 September 2015, *Sérvulo & Associados - Sociedade de Advogados Rl v. Portugal*, Appl. no. 27013/10; ECtHR,, *Sommer v. Germany, op. cit.* (n. 13), para. 56; ECtHR, 17 May 2018, *Wolland v. Norway*, Appl. no. 39731/12, para. 75.↩
35. ECtHR, *Yuditskaya and Others v. Russia*, *op. cit.* (n. 31); also: ECtHR, *Kruglov and Others v. Russia*, *op. cit.* (n. 24), para. 132; ECtHR, *Iliya Stefanov v. Bulgaria*, *op. cit.* (n. 31), para. 43.↩
36. On the search of computers in lawyer's offices, see ECtHR, *Petri Sallinen and Others v. Finland*, *op. cit.* (n. 27); ECtHR, *Wieser and Bicos Beteiligungen GmbH v. Austria*, *op. cit.* (n. 34).↩
37. ECtHR, *Wolland v. Norway*, *op. cit.* (n. 34).↩
38. On this judgment, see L. Bachmaier Winter (2022), "Lawyer-client privilege and computer searches in law offices…", *op. cit.* (n. 32), pp. 275-276.↩
39. ECtHR, 16 November 2021, *Särgava v. Estonia,* Appl. no. 698/19, paras. 99 and 100.↩
40. Ibid. para. 102.↩
41. Ibid. paras. 98 and 103.↩
42. With regard to the lack of safeguards in the seizure of electronic data, see also ECtHR, 3 December 2019, *Kirdök and Others v. Turkey*, Appl. no. 14704/12, paras. 52-57.↩
43. See Guidelines on Digital Forensic Procedures for OLAF Staff, *op. cit.* (n. 6).↩
44. Article 6.3 of the Guidelines, *op. cit.* (n. 6).↩
45. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, 18.↩
46. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, 118. Although the Regulation will be applicable from 18 August 2026 onwards only, certain aspects already affect the right to lawyer-client confidentiality which should be pointed out here.↩
47. See Art. 11(1) lit. a) and Recital 20 DEIO.↩
48. See L. Bachmaier, "Mutual Admissibility of Evidence and Electronic Evidence in the EU – A New Try for European Minimum Rules in Criminal Proceedings?", (2023) *eucrim*, 223-229.↩
49. On the need to establish general principles for transnational criminal proceedings, see J. Vervaele and S. Gless, "Law Should Govern: Aspiring General Principles for Transnational Criminal Justice", (2013) 9(4) *Utrecht Law Rev*., 1-10; see also, S. Gless, *Beweisgrundsätze einer grenzüberschreitenden Rechtsverfolgung*, 2007, pp. 142 ff.↩
50. I only refer to the Production Order, because the Preservation Order (although also entailing interference in data protection rights of a person by ordering the retention of such data until the Production Order is being issued) does not pose problems as to evidence transfer and admissibility.↩
51. Recital 63 EPO/EPRO-Regulation.↩

* Author statement

This article elaborates on previous findings and publications by the author on the topic of the lawyer-client privilege. It was written within the framework of the research project «Proceso penal transnacional, prueba y derecho de defensa en el marco de las nuevas tecnologías y el espacio digital» (PID2019-107766RB-I00), financed by the Spanish Ministry of Science and Innovation.

COPYRIGHT/DISCLAIMER
© 2024 The Author(s). Published by the Max Planck Institute for the Study of Crime, Security and Law. This is an open access article published under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. If users remix, transform, or build upon the material, they may not distribute the modified material. For details, see https://creativecommons.org/licenses/by-nd/4.0/.
Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and “criministrative” law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU’s financial interests – a key driver of European integration in “criministrative” justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union