The right to lawyer-client confidentiality: a plea for common standards in eu cross-border criminal proceedings

O direito à confidencialidade entre advogado e cliente: standards comuns nos processos crime transnacionais

LORENA BACHMAIER WINTER[1]

GALILEU – REVISTA DE DIREITO E ECONOMIA · e-ISSN 2184-1845
Volume XXIV · 1st January Janeiro – 31ST December Dezembro 2023 · pp. 39-56
DOI: https://doi.org/10.26619/2184-1845.XXIV.1/2.3
Submitted on April 1st, 2023 · Accepted on july 31st, 2023
Submetido em 1de Abril, 2023 · Aceite a 31 de julho, 2023

KEYWORDS: lawyer-client; confidentiality; criminal investigations; European Investigation Order.

PALAVRAS-CHAVE: advogado-cliente: confidencialidade; investigações criminais; Ordem Europeia de Investigação.

1 *Catedrática Derecho Procesal. Universidad Complutense Madrid.*

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 39-56

1. Introduction

The European Convention on Human Rights does not expressly guarantee the right of a defendant to communicate confidentially with his defence attorney, but this right is enshrined in the fair trial safeguards of Article 6 ECHR.[2] The Court has been very attentive when it comes to protect this right, and along its case-law the content and scope of the right to lawyer-client confidentiality has been defined. 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 client, and the safeguarding of professional secrecy is the corollary of the right to legal assistance and the right against self-incrimination.[3] The confidentiality of the communications of a person with a lawyer in the context of the legal assistance falls within the scope of private life and the ECtHR has consistently recognized that the right of the accused to communicate with his lawyer without being heard by a third party is one of the core elements of the right to a fair trial in a democratic society.[4] This right is set out in Article 6 (3) (c) ECHR and covers direct oral communications, as well as postal communications, by telephone, or by way of any electronic system.

The aim of this article is to make a plea for the protection of the lawyer-client privilege at the European Union level. 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 entail important risks in transnational criminal proceedings and leading to blatant violations of this right in the context of cross-border evidence gathering.

To advance towards an EU legislative framework, it is important to stake stock of the content of the right to lawyer-client confidentiality in the European landscape and therefore this article will begin presenting an overview of the caselaw of the ECtHR on lawyer client privilege in connection to with the measures adopted in criminal investigations.[6] I will be very briefly summarise the ECtHR case-law about the interception

2 This article elaborates further on previous findings and publications by the author on the topic of the lawyer-client privilege. This article has been written within the 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.

3 On the *lawyer-client privilege* in the USA, see the comprehensive reference book of E. Epstein, *The Attorney-Client Privilege and the Work-Product Doctrine*, ABA Publishing, Chicago, 2017.

4 See for example, ECtHR *S. v. Switzerland*, para. 48; Appl. nos. 12629/87 y 13965/88, 28 November 1991, para. 48.

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*, Cham, Springer 2020.

6 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*, Thomson-Aranzadi, Cizur Menor, 2022, pp. 21-79.

of communications of lawyers, the entry and search in lawyers' offices, and the position of the lawyer as witness against his/her client. At the sight of these standards defined by the Strasbourg Court, some of the problems that might appear in cross-border criminal proceedings regarding the lawyer-client privilege in the gathering of evidence and the executing of European Investigation Orders (EIO) will be pointed out. Finally, I will argue that the European Union law should address the need to effectively protect the right to lawyer-client confidentiality in transnational criminal proceedings.

2. Brief overview of the case law of the ECtHR on the right to lawyer-client confidentiality and the protection against interferences in criminal investigations

The right to confidentiality of the lawyer-client communications is recognized in numerous recommendations of the Council of Europe and resolutions of its Parliamentary Assembly, such as the *Standard Minimum Rules for the Treatment of Prisoners* (Article 93),[7] as well as in the United Nations the *Basic Principles on the Role of Lawyers* adopted in 1990.[8] Council of Europe Recommendation Rec (2000) 21[9] urges the governments of the Member States to take all necessary measures "to ensure the respect of the confidentiality of the lawyer-client relationship. Exceptions to this principle should be allowed only if compatible with the Rule of Law."[10] Further, the CoE Recommendation Rec 2085 (2016) *Strengthening the protection and role of human rights defenders in Council of Europe Member States*[11] also recommends that the members States take actions to strengthen the role of human rights defenders and to increase their protection.[12]

The Court has highlighted that it is clearly in the general interest that any person who wishes to consult a lawyer is free to do so under conditions which favour full

7 Annex to the Resolution (73) 5 of the Committee of Ministers of 19.1.1973, accessible at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804fac9a

8 *Basic Principles on the Role of Lawyers* adopted on 7 September 1990, at the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, La Habana (Cuba); ONU Doc. A/CONF.144/28/Rev.1 p. 118 (1990), para 22: "Governments shall recognize and respect the confidentiality of all communications and consultations between lawyers and their clients, within the framework of their professional relationship."

9 Recommendation (2000)21, *On the freedom of exercise of the profession of lawyer*, adopted by the Committee of Ministers of the Council of Europe, 25 October 2000.

10 See principle I.6.

11 Recommendation Rec 2085 (2016) of 28 January 2016, accessible at: https://pace.coe.int/en/files/22501/html.

12 The Resolution of the Parliamentary Assembly of the Council of Europe 2095 (2016) *Strengthening the protection and role of human rights defenders in Council of Europe member States* of the same date contains the same recommendation. Accessible at: https://pace.coe.int/en/files/22500/html.

and uninhibited discussion.[13] This general interest is not limited to the protection of communications or actions related to pending proceedings, but also to the provision of legal advice in general. Any citizen who goes to a lawyer to consult any legal issue should have the reasonable expectation that his communications are private and confidential.[14]

The right to confidentiality of the lawyer-client communications must be guaranteed in such a way that its exercise is effective and not merely formal. Hence, the European Court of Human Rights has underlined the importance of providing for and complying with the specific procedural guarantees designed to protect the confidentiality of these communications.[15]

Any interception of the communications between lawyer and client in criminal proceedings implies an interference with Article 8 ECHR, which can also entail an infringement of Article 6 ECHR.[16] The Court differentiates on the one hand interferences in the right of Article 8 ECHR because of measures adopted in the context of a criminal investigation; and, on the other hand, the impact that the violation of the right to attorney-client confidentiality may have on the rights guaranteed under Article 6 ECHR.[17]

It should be added that the seizure of a client's documents that are in the possession of his lawyer, and which are obtained without respecting the right to professional secrecy, can also constitute a violation of the right to non-self-incrimination,[18] although it is true that once confirmed that there has been a violation of Article 8 ECHR, the ECHR usually does not assess its impact upon Article 6 ECHR.

Since *Golder v. United Kingdom* and *Niemietz v. Germany*,[19] the Court has been defining the requirements that must be met so that interference in the lawyer-client privilege can be considered in accordance with the Convention. Strasbourg case-law has also extensively addressed the right of the detainee or prisoner to communicate with their lawyer, as a

13 *Campbell v. United Kingdom,* Appl. no. 13590/88, 25 March 1992, para. 46. On the impact of the ECtHR's case law and the *lawyer-client privilege* in the *common law systems*, see J. Auburn, *Legal Professional Privilege: Law and Theory,* Hart, Oxford, 2000, pp. 37 ff.

14 See *Altay v. Turkey* (n. ° 2), Appl no. 11236/06, 9 April 2019, paras. 49-51.

15 See, for example, *Sommer v. Germany*, Appl. no. 73607/13, 27 April 2017, para. 56; *Michaud v. France*, Appl. no. 12323/11, 6 December 2012, para. 130.

16 On this issue, see generally T. Spronken, J. Fermon, "Protection of Attorney-Client Privilege in Europe", *Penn State International Law Review,* vol. 27, Nr. 2-2008, pp. 439-463.

17 For instance, if a lawyer could not meet with his client and receive confidential instructions from him without being overheard, the right to legal assistance would be deprived of its purpose. See *Golder v. United Kingdom,* Appl. No. 4451/70, 21 February 1975 (para. 45); *M. v. The Netherlands*, Appl. no. 2156/10, 25 July 2017, para. 85. In the latter case, the ECHR deals with the possible violation of Article 6.3.c) ECHR in a matter related to the disclosure of classified information and the restrictions on access to a lawyer and to communicate confidentially in a case involving state secrets and national security interests.

18 See *André & Others v. France*, Appl. no. 18606/03, 27 July 2008, para. 41.

19 *Niemietz v. Germany*, Appl. no. 13710/88, 16 December 1992; *Kolesnichenko v. Russia,* Appl. no. 19856/04, 9 April 2009.

substantial part of the right to defence and the right to legal assistance.[20] Although this is a very important aspect of the protection of the confidentiality of communications, I will not address here the communications with the detainee but will focus on problems arising from criminal investigative measures in the gathering of evidence.

2.1 Interception of telephone communications

The right to defense and legal assistance would not be effective without the protection of the confidentiality of the lawyer-client communications. Although not all conversations between the lawyer and his/her client are protected by the lawyer-client privilege, all legal systems provide for the strict prohibition to intercept the telephone of the lawyer who is not charged, because Article 8 ECHR protects the confidentiality of any "communication" but it grants a reinforced protection to communications between lawyers and their clients.[21]

Although there are cases where the telephone of a lawyer is directly tapped without respecting the minimum safeguards for the professional secrecy –especially in countries where the principles of the rule of law are not respected[22]–, in practice the major problem arises from the communications that are accidentally intercepted when the defendant's telephone is tapped, or his/her computer is searched.[23] Indeed, it is generally recognized that it is almost impossible to prevent some of those conversations from being overheard or even recorded. Precisely, when the conversations are in another language or the interlocutors are not identified, it will be difficult to know at the time of recording that the privileged communication between lawyer and client is being intercepted.

This was already stated in the benchmark case *Kopp v. Switzerland*,[24] a case dealing with the interception of the telephone of the law office of Mr. Kopp, whose telephone was tapped in relation with the investigation of a leak of secret information of the department of justice, where his wife was working. Even if Mr Kopp was being investigated in another criminal procedure for money laundering, the wiretapping was not ordered within such investigation, Mr Kopp was thus a non-suspect lawyer in this case. Although the case

20 *Golder v. United Kingdom*, Appl. No. 4451/70, 21 February 1975; *Schönberger and Durmaz v. Switzerland*, Appl. No. 11368/85, 20 June 1988; *Castravet v. Moldova*, Appl. no. 23393/05, 13 March 2003; *Sarban v. Moldova*, Appl. no. 3456/05, 4 October 2005; *Khodorkovskiy v. Russia*, Appl. no. 5829/04, 31 May 2011; *Laurent v. France*, Appl. no. 28798/13, 24 May 2018.

21 Vid. *R.E. v. United Kingdom*, Appl. no. 62498/11, 27 October 2015, para. 131; or *Dudchenko v. Russia*, Appl. no. 37717/05, 7 November 2017, para. 104.

22 As noted in *Kadura and Smaliy v. Ucrania*, Appl. nos. 42753/14 and 43860/14, 21 January 2021.

23 Vid. L. Bachmaier Winter, "Intervenciones telefónicas y derechos de terceros en el proceso penal", *Revista de Derecho Procesal*, nos. 1-3, (2004), pp. 50 ff.

24 *Kopp v. Suiza*, Appl. no. 13/1997/797/1000, 25 March 1998.

at the end was analyzed from the perspective of insufficient legal provision, the Court highlighted the difficulty in avoiding privileged communications to be intercepted.[25]

Similarly in the case of *Pruteanu v. Romania*[26], the Strasbourg Court was confronted with a complaint filed by a lawyer whose conversations with his client had been accidentally recorded and decided also on the grounds of insufficient legal provision in the national law. Thus the Court, aware of the impossibility to prevent in many cases such accidental interceptions of privileged communications, puts the focus on the need for an adequate legal regulation providing for safeguards, such as the destruction of the recordings. However, the Court does not go so far as to establish that the privileged communications should be excluded as evidence in case they finally were to reach the trial. The Court does not impose exclusionary rules of evidence to the Member States in this context,[27] and has even declared that the use of such privileged communications as evidence is not contrary to Article 8 ECHR when the lawyer himself was accused by the client for revealing confidential information.[28]

2.2. Entry, search and seizure in lawyer's offices

Many legal systems only authorize the entry and search of a law firm, when the lawyer himself is the suspect, [29] but most of them will allow this measure, even if the lawyer is not the suspect. However, the ECtHR has taken a much stricter approach when the search is carried out in the office of a lawyer who is not a suspect,[30] requiring "compelling reasons" to justify such interference in Article 6 and eventually Article 8 ECHR.[31] When there is an adequate and sufficient legal provision, the objective pursued is legitimate

25 See also *Vasil Vasilev v. Bulgaria,* Appl. no. 7610/15, 16 de November 2021, where the communications between the investigated suspect –an ex Minister of Defence– and his lawyer where accidentally recorded, since the suspect's phone was tapped. The lawyer filed the complaint before the ECtHR claiming that he was entitled to damages for this unlawful interference into his right to privacy. The case was also decided based on lack of sufficient legal provision, because Bulgarian law did not establish how to proceed in those cases where the lawyer-client communications had been accidentally recorded (para. 94).

26 *Pruteanu v. Rumania,* Appl. no. 30181/05, 3 February 2015.

27 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*, Cham, Springer 2020, pp. 101 and 104.

28 In this sense, see *Versini-Campinchi and Crasnianski v. France*, Appl. no. 49176/11, 16 June 2016.

29 This is the case, for example, in Portugal and in several States of the U.S., precisely Oregon and Minnesota. See L. Bachmaier and S. Thaman, "A Comparative View of the Right to Counsel and the Protection of Attorney-Client Communications", cit., p. 55.

30 This was the case in *Roemen and Schmit v. Luxembourg,* Appl. no. 51772/99, 25 February 2003. See also, *Kruglov and Others v. Russia*, Appl. no. 11264/04 *et al*., 4 February 2020, para. 128.

31 *Khodorkovskiy and Lebedev v. Russia*, Appl. no.11082/06, 13772/05, 31 May 2011.

and meets the requirement of necessity and proportionality, and the search is carried out respecting the adequate safeguards, the ECtHR has accepted such measures. [32]

In the case law of the Court, most judgments that find a violation of Article 8 ECHR are based on the lack of a sufficient legal provision, and specifically, because the legal framework did not provide for specific safeguards to protect the lawyer-client confidentiality.[33] According to the Court[34] the law shall specify who shall execute the measure and the way 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 foreseen, the Court proceeds to check whether these legal safeguards have been effectively implemented during the search and seizure of the lawyer's office. In particular, the ECtHR has paid special attention to the following circumstances.

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

This is not a mere formality,[35] and to comply with the Convention the limitation of the scope of the search and seizure must be clear, especially when it comes to computer searches and access to electronic files, in order to ensure the principle of proportionality.[36] The Court does not require in any event an *ex ante* judicial order authorizing the search in a law firm, but for the measure to be in accordance with the Convention, in cases where no prior judicial warrant was issued, there must be the possibility to check the content and adequacy of the measure already agreed upon, by way of an *ex post* judicial decision, as was stated in the *Smirnov v. Russia* case.[37] 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 to be relevant

32 See *Tamosius v. United Kingdom*, Appl. no. 62002/00, 19 September 2002, inadmissibility decision in a tax fraud case. See also *Brito Ferrinho Bexiga Vila-Nova v. Portugal*, Appl. no. 69436/10, 1 December 2005; *Sorvisto v. Finland*, Appl. no. 19348/04, 13 January 2009, para. 118; *Heino v. Finland*, Appl. no. 56720/09, 15 February 2011, para. 43.

33 See, for example, *Petri Sallinen and others v. Finland*, cited above. See extensively, L. Bachmaier, "Lawyer-client privilege en la jurisprudencia del Tribunal Europeo de Derechos Humanos" (2022), cit., p. 22 ff.

34 *Saber v. Norway*, Appl. no. 459/18, 17 December 2020.

35 See *Kruglov and Others v. Russia*, Appl. no. 11264/04 *et al.*, 4 February 2020.

36 In any event, the frequent practice of cloning or mirroring of the entire hard drive, both in direct computer searches as well as in remote computer searches, will inevitably lead 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, "Registro remoto de equipos informáticos y principio de proporcionalidad en la Ley Orgánica 13/2015", *Boletín de Información del Ministerio de Justicia*, no. 2195 (enero) 2017, pp. 3-33, pp. 10 ff.

37 *Smirnov v. Russia*, Appl. No. 71362/01, 7 June 2007, para.47. See also *Heino v. Finland*, 15 February 2011.

to the ongoing criminal investigation, such broad authorization is not compatible with the guarantees that must be respected to protect the professional secrecy and therefore it constitutes a violation of Article 8 ECHR.[38]

2) Whether the necessary safeguards were adopted to protect professional secrecy during the search and seizure.

These safeguards include the process of separating privileged documents or materials, so that they are not seized and the officers could not access them, that the search is carried out in the presence of the lawyer and he/she has the chance to identifying those documents protected by the right to confidentiality and ensure that the seized elements are not disproportionate; and the presence of an independent observer who can control that the files protected by professional secrecy are not seized.[39] In some cases, the Court has taken into account the presence of a judge during the search, supervising that it complies with the court order, as a reinforced safeguard. [40]

Indeed, the presence of an independent third party with sufficient qualifications to control that materials or documents protected by professional secrecy are not seized is one of the safeguards that the ECtHR considers when deciding on the conformity with the Convention of the entry and search in a law firm, becoming therefore an almost absolute requirement, as seen in the cases of *Roemen and Smit v. Luxembourg*; [41] *Wieser and Bicos Beteiligungen GmbH v. Austria*;[42] *Andre and Another v. France*;[43] *Jacquier v. France*;[44] *Xavier Da Silveira v. France*;[45] *Sérvulo & Associados – Sociedade de Advogados Rl v. Portugal*;[46] *Sommer v. Germany*;[47] or in *Wolland v. Norway*.[48]

38 *Robathin v. Austria*, Appl. no. 30457/06, 3 July 2012, paras. 47, 51, 52. See also *Iliya Stefanov v. Bulgaria*, Appl. no. 65755/01, 22 May 2008; *Leotsakos v. Greece,* Appl. no. 30958/13, 4 October 2018, paras. 43, 52; or *Yuditskaya y Otros v. Russia*, Appl. no. 5678/06, 12 February 2015.

39 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*, Giapichelli, Torino, 2022, pp. 261-286, pp. 267 ff.

40 See *Tamosius v. United Kingdom*, Appl. no. 62002/00, 19 September 2002.

41 *Roemen and Smit v. Luxembourg,* Appl. no. 51772/99, 25 February 2003, para. 69.

42 *Wieser and Bicos Beteiligungen GmbH v. Austria*, Appl. no. 74336/01,16 October 2007.

43 *André and Another v. Francia* Appl. no. 18603/03, 24 July 2008, paras. 42 y 43.

44 *Jacquier v. France*, Appl. no. 45827/07, 1 September 2009, where the Court considered that the presence of the dean of the Bar Association during the search was a relevant factor to consider when deciding whether there had been a violation of Article 8 ECHR.

45 *Xavier Da Silveira v. France*, Appl. no.43757/05, 21 January 2010, paras. 37 and 43

46 *Sérvulo & Associados – Sociedade de Advogados Rl v. Portugal*, Appl. no. 27013/10, 3 September 2015.

47 *Sommer v. Germany,* Appl. no. 73607/13, 27 April 2017, para. 56.

48 *Wolland v. Norway*, Appl. no. 39731/12, 17 May 2018, para. 75.

In the case of *Yuditskaya and Others v. Russia*,[49] the search was carried out in the presence of the lawyer and two witnesses, as required by Russian law at the time. The Court understood that the presence of these two witnesses cannot be considered as a sufficient safeguard of the right to professional secrecy, since they did not have any kind of legal training or knowledge, so they were not able to identify which documents or material were covered by professional secrecy. The ECHR ruled in the same terms in the *Kruglov v. Russia*, confirming that the presence of two witnesses is not a sufficient safeguard for the protection of the right to professional secrecy;[50] and also in *Iliya Stefanov v. Bulgaria*, 22 May 2008 (para. 43).

As to the safeguards that have to be adopted to protect the files and communications subject to lawyer-client privilege to be in accordance with the Convention, the Court has laid down some guidelines on the manner and conditions on which searches in law firms must be carried out,[51] although in practice this measure continues to raise concerns — especially the search and seizure of computers and electronic files—, because most legal systems do not contain detailed rules. It often occurs that the judicial warrant authorizing the search and seizure only specifies the type of documents that are sought and can be seized, but not which are the keywords or the search programs to be used to identify the files protected by the lawyer-client privilege. The case of *Wolland v. Norway*[52] is interesting as it shows the detailed procedure to be followed according to the Norwegian legislation in cases of search of computers and all the safeguards provided to prevent that privileged documents and communications are accessed and seized.[53]

Furthermore, while 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 the designated premises to carry out the examination in the forensic laboratory by public IT officers or by an independent computer team.

49 *Yuditskaya and Others v. Russia*, Appl. no.5678/06, 12 February 2015.

50 *Kruglov and Others v. Russia*, para. 132. It is interesting to note that in 2017 and, as a result of a ruling by the Constitutional Court of that country on December 17, 2015, a reform of the Russian Criminal Procedure Code was undertaken in which, among others, the rules related to search of lawyers' offices were amended. Specifically, the new Article 450.I CPP contemplates the requirement of the presence of a representative of the bar association during the search and seizure.

51 On the search of computers in lawyer's offices see *Petri Sallinen and others v. Finland*, Appl. no. 50882/99, 27 September 2005; *Wieser and Bicos Beteiligungen GmbH v. Austria*, Appl. no. 74336/01,16 October 2007.

52 *Wolland v. Norway*, 17 May 2018, paras. 8 to 11.

53 On this judgment see, 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", cit., pp. 275-276.

In the case of *Särgava v. Estonia*,[54] dealing with the search of electronic devices of lawyers, the ECtHR made a very clear statement, stating that the documents protected by lawyer-client privilege need to be separated from the files that are not covered by professional secrecy, and this safeguard is of outmost importance when it comes to electronic data and search of electronic devices:

> "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." (para. 99)
>
> "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." (para. 100)

The Court acknowledges that cloning the device might be necessary to prevent illicit tampering with the device, and it also allows the devices to be quickly returned to their owner. But, in this case, measures must be adopted to guarantee that during the copying and screening of the content of the devices, data not covered by the judicial authorization cannot be accessed and safeguards must be in place to prevent privileged data to be accessed and seized.[55]

In this case, the Court took into consideration that the judicial order did not specify the measures to be adopted to protect professional secrecy, even though it was already known that protected documents were stored in the seized devices. The national legislation did not establish the procedure to be followed in the access to electronic data nor did it contemplate specific measures so that during the examination of the devices the protection of professional secrecy would be guaranteed (paras. 98 and 103).[56] And even though the search of the devices was limited using more specific search terms, that way of proceeding was not foreseen in the prosecution's request or in the court order but was

54 *Särgava v. Estonia*, Appl. no. 698/19, 16 November 2021.
55 Para. 102.
56 With regard to the lack of safeguards in the seizure of electronic data see also *Kirdök and Others v. Turkey*, Appl. no. 14704/12, 3 December 2019, paras. 52-57.

GALILEU · e-ISSN 2184-1845 · Volume XXIV · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2023 · pp. 39-56

a decision of the investigators themselves. In addition, the person under investigation did not participate nor was present during the choosing of the search terms and the selection of the files to be examined in the criminal proceeding (para. 106).

At this point, the Court makes a statement that I consider very relevant to establish a violation of the Convention: it is not enough that specific measures were adopted to limit the search to avoid a violation of the Convention. The fact that such safeguards were not foreseen in the law prevented the affected party from challenging the legality of the search and seizure carried out. And in 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 these privileged documents from being downloaded and read by investigators once the computers have been seized, in view of the Court, it already constitutes a violation of the Convention. The absence of a legal regulation with specific provisions on the handling of the electronic files and the sifting of the privileged documents, led the Court to consider that the examination of the content of the laptop of the lawyer Mr. Särgava infringed Article 8 of the ECHR even if in practice this measure was executed adequately, respecting the principle of proportionality after a sound sifting of the files.

2.3. Lawyer summoned as witness against the client

There are only a few cases where the ECHR has faced the question of the scope of the lawyer's professional secrecy in relation to the obligation to testify as a witness in criminal proceedings, since most legal systems exclude this possibility. For this reason, it is important to reflect with some detail on the facts and the arguments of the ECtHR in the case of *Klaus Müller v. Germany,*[57] dealing with the question of who the owner of the right to professional secrecy is, and thus who can waive it.

Klaus Müller's firm had provided legal services to four companies over eighteen years in connection with various legal transactions. The four companies entered insolvency proceedings in 2014 and in 2017 criminal proceedings were instituted against the executive directors of each of the companies, among others, for the crime of fraud. In this criminal proceedings, Klaus Müller, who does not represent any of the defendants, is summoned to testify as a witness regarding some of the sales and other transactions on which he had advised companies in the past. The current CEO of the four companies, as well as the bankruptcy administrator relieve Müller of his obligation to keep professional secrecy. Müller, however, refuses to testify, because he understands that to do so, the

57 *Klaus Müller v. Germany*, Appl. no. 24173/18, 19 November 2020.

four defendants who held the positions of executive director of the companies at the time he provided his legal services should also renounce professional secrecy. His refusal to testify results in the court imposing an administrative penalty of 150 euros, a penalty that is confirmed on appeal and increased up to 600 euros.[58]The question that arises is whether the lawyer was hired by the company and provided his services to it, in which case it would be sufficient that the current director of the company –in addition to the bankruptcy administrator– released the lawyer from the obligation of professional secrecy; or whether the legal services had been commissioned by both –the company and its executive directors in a personal capacity–, in which case the authorization of the four directors would be required to revoke the obligation to keep professional secrecy. Without entering more details, it must be pointed out here that at the national level the jurisprudence of the different German courts was not uniform and that the appeal filed before the Federal Constitutional Court was not admitted.

Müller filed a complaint before the ECtHR stating that the sanction for complying with his obligation to keep professional secrecy was against Article 8 of the Convention. The ECtHR however, followed the position adopted by the German court of appeal, which considered that the legal services provided by Müller had been commissioned by the companies; and since the company had renounced that privilege through its current director, Müller was obliged to testify as a witness (para. 69). On this basis, the ECtHR decided that there had been no violation of Article 8 ECHR. The Court, however, skipped the question of who the owner of the right to professional secrecy is, invoking the doctrine of the national margin of appreciation (para. 66).[59]

This decision is highly relevant since it establishes that the waiver of the client-attorney privilege does not require the consent of the natural persons who have acted on behalf and in the interest of the company at the time the legal advice was given, and the investigated events occurred. According to the ECtHR, it is enough for the privilege to be waived by the current representative or the insolvency administrator.[60]

58 Differently from the Spanish approach, where the professional secrecy is considered both, a right and an obligation (art. 542.3 LOPJ). See J. Rico Balbona, *El secreto profesional de los abogados y procuradores en España*, Bosch, Barcelona, 1988, pp. 16 ff.

59 The dissenting opinion to the Court's decision in this case, underlines that the national legal law lacked clarity – shown by the existing divergent jurisprudence at the national level– and, that the directors, although acting on behalf of the company, were *de facto* clients of the lawyer summoned as witness. Upon these facts, the dissenting judge considers that the lawyer was bound by the duty of confidentiality regarding the communications maintained with them.

60 See the USA Supreme Court judgment, *Commodity Futures Trading Commission (CFTC) v. Weintraub,* 471 US 343 (1985). For Germany, see E. Corbo, *Strafprozessuales Zeugnisverweigerungsrecht für Insolvenzverwalter?*, Peter Lang, Berlin, 2020.

Although this conclusion might be seen as logical, even more so when there was no personal contractual relationship between the lawyer and the directors of the accused company, it is also true that there are arguments to support the opposite conclusion. Being the professional secrecy a core right of the right to legal assistance and the right to defense, in balancing the obligation to testify and the obligation to keep professional secrecy –when there are doubts about whether the lawyer has been released from it or not–, in my opinion the ECtHR should have prioritized the lawyer-client confidentiality. Certainly, more solid arguments would have been expected, and certainly stating that the national law in this case was clear (para. 57) –when at the national level albeit in different Länder there is contradictory jurisprudence, is not fully convincing.[61]

Finally, using the inadmissibility decision of the German Constitutional Court as an argument that the sanction imposed to the lawyer for refusing to testify against the company, was in conformity with the Convention, is also doubtful.[62]

The rule on the admission of the appeal before the *Bundesverfassungsgericht* (Article 93 a) *BVerfGG Annahme von Verfassungsbeschwerden*) provides that the appeal before the Constitutional Court must be admitted if the matter has constitutional relevance or if, in the cases of Article 90 *BVerfGG*, the inadmissibility would cause especially serious damage to the appellant. To consider the inadmissibility decision, which is not motivated, as an additional argument for the ECtHR to decide against the lawyer, does not seem to be consistent.[63]

3. Lawyer-client privilege and the European Investigation Order

As is well-known, the Directive on the EIO combines the principle of mutual recognition with the system of mutual legal assistance, which provides flexibility to this instrument, while reducing the automatic execution of the request. This explains that the Directive –and the transposition laws in the Member States– provide for a detailed list of grounds

61 Vid. para 57: (…) no legal uncertainty arose for the applicant from the fact that some other courts of appeal in different areas of territorial jurisdiction interpreted the scope of the right not to testify in circumstances such as those in the present case in a different manner."

62 See para. 54: "*The Federal Constitutional Court, by declining to consider the applicant's constitutional complaint, albeit without giving reasons, appeared to consider that the approach taken by the domestic courts in the applicant's case did not raise an issue under the German Constitution.*"

63 Vid. C. Lenz and R. Hansel, "Paragraph 93", *Bundesverfassungsgerichtsgesetz. Handkommentar,* Nomos, Baden-Baden, 2020.

for refusal, which are mainly regulated in Article 11, but also in Article 10 ("Recourse to a different type of investigative measure"), among others.[64]

When it comes to the grounds for refusal, Article 11 DEIO, includes a long list of possible grounds for refusal, which have been transposed by most Member States as mandatory grounds for refusal. Among those, Article 11 (1) EIO mentions the existence of an immunity or a privilege under the law of the executing State as a possible ground for refusal.[65] Recital (20) of the Explanatory Memorandum of the DEIO states that "there is no common definition of what constitutes an immunity or privilege in Union law; the precise definition of these terms is therefore left to national law." As examples, it cites "protections which apply to medical and legal professions" but explaining that these are not the only ones that could come into consideration and that this provision "should not be interpreted in a way to counter the obligation to abolish certain grounds for refusal as set out in the Protocol to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union".

With regard to the measure of search and seizure in a lawyer's office, the first question that arises is whether it constitutes a ground for refusal under Article 11 (1) (a) of the DEIO and thus the executing State should simply invoke the existence of such privilege to refuse its execution; or on the contrary, that the executing authority cannot refuse to execute such measure, because it exists under domestic law. In those member States where the entry and search of a lawyer's office can only be carried out when the lawyer himself is the suspect or accused, the measure would be refused under 10 (1) (b) DEIO (the measure would not be available in a similar domestic case). But, in all other cases, in principle, as the measure exists, the fact that privileged materials could not be seized, should not lead to the refusal to execute the EIO.

This being said, the next question relates to the way such search and seizure should be carried out, so that the executing State respects its own procedural rules, and at the same time, complies with *lex fori*, to ensure that the evidence gathered will be admissible as evidence.

As can be seen from the case-law of the ECtHR and has been also confirmed in comparative studies, there is no harmonization on how to proceed with regard to the

64 A substitution can also take place when the same results as the measure requested in the EIO could be achieved by less intrusive means. However, in those cases where the requested measure is not available, and its substitution is not possible or would not have the same results the executing authority may refuse its execution. See L. Bachmaier Winter, "The role of the proportionality principle in the cross-border investigations involving fundamental rights", in S. Ruggeri (ed.), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings*, Ed. Springer, Heidelberg, New York, 2013, pp. 100-101.

65 See Article 11 (1) (a) DEIO.

safeguards for the filtering of privileged and non-privileged communications in the context of interception of communications as well as in the case of searches of computers. Furter, the exclusionary rules of evidence among the EU Member States also diverge from each other, thus the effective protection of the lawyer-client privilege might become completely ineffective when, 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 admissibility of evidence in criminal proceedings have been pointed out several times:[66] 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 the procedural safeguards and the rights of the defence.[67] This is a situation that is not originated by the EIO Directive, but from the interplay of different legal systems, when gathering evidence by way of international judicial cooperation. The issue that arises here is how to protect the fundamental right to the confidentiality of the 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*? According to which rules?

In practice, the issuing authority requesting a search and seizure in a precise home or address, does not even know that it is a law office or the private home of a lawyer (and often the office is a room which is part of the home). In such cases, the execution of the EIO should be halted, and further information should be asked to the issuing State. At that point, if the issuing authority asks for the computer to be cloned, or even sent over to the issuing State, which are the applicable rules to prevent that lawyer-client privilege is infringed? Who is to ensure it?

In that context, which standards should the trial court take into account to determine whether the search and seizure in a lawyer's office carried out in another member State by way of an EIO, does not infringe the fundamental rights as defined by the ECtHR? Let us take following example: in execution of an EIO, the authorities of the foreign State enter a lawyer's office and search several computers and seize some electronic files, in accordance with the scope of the search defined in the judicial order that gives rise to the

66 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", *Utrecht Law Rev.,* vol.9, issue 4 (Sept.) 2013, pp. 1-10: there is "need of rules that comprehensively deal with transnational criminal cases", p. 10.

67 S. Gless, *Beweisgrundsätze einer grenzüberschreitenden Rechtsverfolgung*, pp. 142 ff.; I. Zerbes, "Fragmentiertes Strafverfahren. Beweiserhebung und Beweisverwertung nach dem Verordnungsentwurf zur Europäischen Staatsanwaltschaft", *ZIS* 3/2015, pp.145-155, although this last one referring specifically to the criminal proceedings under the EPPO.

issuing of the EIO. However, neither the EIO nor the issuing judicial authority specify the keywords to be used or the way in which the data should be sifted to prevent an unlawful interference into the right to the lawyer-client confidentiality. The executing State follows its own protocols, which are not provided in a legal provision, and thus would fail to comply the standards of the ECtHR. Would the evidence obtained in such way, lacking in the executing State a sufficient legal basis and thus in violation of the ECHR be admissible as evidence in the forum State? The general rule is that if *lex loci* has been complied, the evidence should be admissible in the forum State. However, this general principle on cross-border evidence, has an exception: when the evidence has been obtained in violation of human rights. And, according to the ECtHR, when the safeguards to prevent interference in the lawyer-client privilege are not sufficiently regulated in the law, this is against the Convention, and thus, in violation of human rights.

Another example may illustrate some of the problems that may arise in executing the measure of search and seizure in law offices, in the absence of common rules in the EU Member States. In a case where the judicial order in the issuing State defines the existing suspicions against the lawyer, as well as the scope of the materials that are to be searched, because they are linked to the criminal investigation. But the court order does not indicate the executing authority which key words should be used in the search of the computer. The executing authority proceeds to use the keywords they consider appropriate and end up with a disproportionate number of files searched and seized, as it happened in the *Sérvulo* case, described above. All those files are sent to the issuing authority. Would that evidence be admissible in the forum State, despite being disproportionate? Or, according to the position followed by the Strasbourg Court, evidence would be admissible as long as the adequate safeguards (presence of an independent observer, possibility to challenge the execution of the measure, oversight by an investigating judge, etc.) were adopted in the executing State? The overbreadth of the search should lead to the exclusion of the evidence obtained in breach of the principle of proportionality. However, as the ECtHR has admitted that the quantity of the files searched and seized is not *per se* contrary to the Convention, as the counterbalancing safeguards adopted to protect the right to lawyer-client confidentiality are also relevant, should the trial court check which were the measures adopted in the executing State to prevent the professional secrecy to be infringed?

Finally, how shall the trial court deal with the files sent from the executing State, when some of them contain privileged materials or communications? Should the receiving authority simply exclude them, and thus carry out the sifting in the issuing State, or would this circumstance already lead to the exclusion of all the evidence transferred?

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

And in legal systems, like the Spanish system, where evidence obtained in breach of fundamental rights falls under the exclusionary rule (Article 11 Judiciary Act), the seizure and transfer of files protected under the lawyer-client privilege would render the whole set of materials seized as inadmissible and assessing such evidence would be against the rule of law. However, for evidence obtained abroad, usually the principle of non-inquiry will be applied. The same applies to many other Member States, as for example Austria which also follow the principle of non-inquiry. On the other hand, if there is a check on how the evidence has been obtained abroad, it will not necessarily lead to the exclusion of evidence, as several countries, as e.g. The Netherlands or Germany, apply a balancing test.[68]

In those States, the assessment of such evidence would be in conformity with Article 6 TUE and with the ECHR, as it does not impose an exclusionary rule of evidence when the lawyer-client privilege has been infringed. Moreover, the EIO Directive only states that the trial court should pay attention to the way the evidence was obtained in the foreign country when assessing the evidence obtained from abroad.

These are only some examples of the problematic questions that arise in the execution of measures of search and seizure, where the right to lawyer-client privilege is not adequately protected, or the rules in the executing State do not provide for sufficient safeguards to prevent this right to be infringed.

4. Concluding remarks

While the right to lawyer-client confidentiality has been recognized for a long time as a fundamental right enshrined in the right to legal assistance and the right of defence, its practical implementation has not been subject to adequate safeguards. The proof of this is the lack of rules at the legislative level in many EU Member States on how to ensure that during the interception of communications and the search of computers, the privileged communications are not seized. The digitalization of society and its communications has stressed the need to implement specific safeguards to prevent unlawful access to

68 On the problems stemming from the lack of rules on admissibility of evidence obtained abroad, see the interesting contribution of S. Gless, "Transnational Cooperation in Criminal Matters and the Guarantee of a Fair Trial: Approaches to a General Principle", *Utrecht Law Rev.*, vol.9, issue 4 (Sept.) 2013, pp. 90-108, 95-96.

materials protected by professional secrecy through investigative measures that encroach in such right. As seen above, the ECtHR has been called to rule on numerous occasions on the right to lawyer-client confidentiality, and in most cases the Strasbourg Court has upheld the claim, finding a violation of the Convention, mostly under Article 8 ECHR.

The majority of the applications before the ECtHR have been granted on the basis of the lack of a sufficient legal provision, requiring a high degree of specificity in the law: not only must there be a legal basis to carry out an interference in the rights protected by Article 8 ECHR but the law must specify in detail the process to be followed in the execution of the interception of communications and also the search and seizure, in order to prevent the violation of the right to lawyer-client confidentiality. Such safeguards must be regulated in detail, on the one hand to avoid arbitrariness or abuses on the part of the public authorities, but also for the citizens to know under which conditions an intrusion into their rights can take place and, therefore when they can challenge such measures.

Lawyer-client privilege may play a relevant role in the execution of an EIO, in the protection of the fundamental rights of the defendant, and in the admissibility of cross-border evidence. By providing an overview of the caselaw of the ECtHR our aim has been to help in identifying what are the common standards on the protection of the fundamental right to confidentiality of the lawyer-client relationship that should be regulated at the European level, by way of a future Directive. It is not enough to draw attention to the need to ensure the protection of the lawyer-client privilege, this right should be effectively protected also in the cross-border gathering of criminal evidence. And to that end, supranational legislative action, to my mind, is needed. Here is the plea for such European legislative framework.