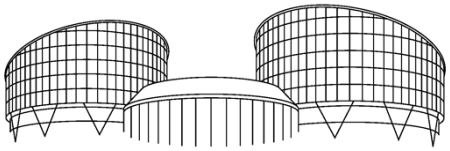

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

THIRD SECTION

CASE OF SÄRGAVA v. ESTONIA

(Application no. 698/19)

JUDGMENT

Art 8 • Correspondence • Lack of sufficient procedural safeguards to protect privileged data during the seizure and subsequent examination of a lawyer's laptop and mobile telephone • Interference not in accordance with the law

STRASBOURG

16 November 2021

FINAL

16/02/2022

This judgment has become final under Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Särgava v. Estonia,

The European Court of Human Rights (Third Section), sitting as a Chamber composed of:

Georges Ravarani, *President,*
Georgios A. Serghides,
Dmitry Dedov,
Darian Pavli,
Peeter Roosma,
Anja Seibert-Fohr,
Andreas Zünd, *judges,*
and Milan Blaško, *Section Registrar,*

Having regard to:

the application (no. 698/19) against the Republic of Estonia lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by an Estonian national, Mr Viktor Särgava ("the applicant"), on 17 December 2018;

the decision to give notice to the Estonian Government ("the Government") of the complaint under Article 8 of the Convention concerning the seizure and examination of the applicant's (a lawyer's) laptop and mobile telephone;

the parties' observations;

the decision to uphold the Government's objection to examination of the application by a Committee;

Having deliberated in private on 12 October 2021,

Delivers the following judgment, which was adopted on that date:

INTRODUCTION

1. The main issue in the present case is whether the domestic law was sufficiently clear and afforded the requisite safeguards for the protection of legal professional privilege in the event of the seizure and subsequent examination of a lawyer's laptop and mobile telephone.

THE FACTS

2. The applicant was born in 1982 and lives in Tallinn. He was represented by Mr T. Lindma, a lawyer practising in Tallinn.

3. The Government were represented by their Agent, Ms M. Kuurberg, of the Ministry of Foreign Affairs.

4. The facts of the case, as submitted by the parties, may be summarised as follows.

I. THE SEARCH AND SEIZURE

5. The applicant is a lawyer (*advokaat*) and a partner in a law firm.

6. The Government asserted that the applicant also worked as an entrepreneur alongside his professional activity as a lawyer. He had been a member of the board and/or a shareholder in a number of companies. He had, *inter alia*, been a shareholder in company S, initially as a natural person and later through another company L. The Government added that according to the criminal suspicion those companies had been under the control of the leaders of a criminal organisation and were linked to the suspicion raised against the applicant.

7. On 26 October 2016 the Police and Border Guard Board (hereafter "the PBGB") initiated criminal proceedings against an alleged criminal organisation and concerning money laundering. The applicant was suspected, *inter alia*, of belonging to a criminal organisation. According to the suspicion, the applicant's role, as someone with a legal background, was to manage the companies linked to the criminal organisation, to draw up the relevant documents and to ensure that the related transactions were legally correct. He was also suspected, in relation to company S, of using a counterfeit document and providing aid in an attempt to cause insolvency.

8. On 12 February 2018, in the course of the aforementioned proceedings and at the request of the State Prosecutor, the preliminary investigation judge *(eeluurimiskohtunik*) of the Harju County Court authorised a search of the applicant's law firm and a search of his home and vehicles, and also ordered the applicant's detention as a suspect for forty-eight hours. The present application concerns the items seized during the search of the applicant's home and car.

9. The State Prosecutor, in the request to authorise a search of the applicant's home and vehicles, noted that the applicant had allegedly been involved in drawing up documents related to criminal activities. The request entailed a detailed description of the criminal activities of which the applicant was suspected. Among other aspects, it mentioned that the applicant was a shareholder in company S.

The State Prosecutor asked the court to authorise a search in order to secure relevant information on communications and transactions between the members of the criminal organisation in hard copy as well as in electronic form. The request referred to various data carriers (*andmekandjad*) such as USB sticks, memory cards, hard drives, and also electronic devices, such as computers and telephones. The State Prosecutor first specifically listed the companies (including the company S), the natural persons and circumstances in relation to which information was sought, adding that "in addition to the aforementioned material, other documents, correspondence and items that might entail evidentiary information in the criminal case" would also be sought. The State Prosecutor pointed out that

having regard to material gathered hitherto in the criminal proceedings and to general criminological information, there were grounds to believe that the information wanted might be found at the applicant's home and vehicles.

The State Prosecutor admitted that in addition to the information relevant to the criminal proceedings, the applicant might have information that related to his professional activities as a lawyer and that would thus not be of relevance to the criminal proceedings.

10. The preliminary investigation judge authorised the search in the extent requested by the State Prosecutor by way of endorsement (*pealdis*, see paragraph 31 below). In the case at hand this meant that no separate court decision was drawn up, but the judge's authorisation was inserted in the "resolution" section of a computer programme used for signing documents digitally. The authorisation stated "Under Article 91 of the Code of Criminal Procedure the preliminary investigation judge authorises a conduct of a search in Viktor Särgava's residence on address X, as well as in its auxiliary buildings and rooms and in cars Y and Z used by Viktor Särgava in order to find the objects mentioned in the prosecutor's request."

11. On the morning of 13 February 2018 the applicant was detained and his mobile telephone was seized from his car. A detention report was drawn up. It was noted in the report that the seized mobile telephone had been placed in an antistatic bag and sealed by a numbered security sticker. The applicant had been informed that, if necessary, information concerning his social media accounts, correspondence and cloud storage could be downloaded from the Internet. The applicant noted that he had read (*tutvunud*) the report and signed it. He did not add any remarks or comments concerning the procedural measures related to his detention.

12. On the same day a search was carried out in the applicant's home. His wife and a lawyer appointed by the applicant were present during the search, while the applicant himself attended the search taking place in his law firm (see paragraph 13 below). The applicant conducted a telephone conversation with his lawyer during the search. The applicant's wife stated that in her view the objects sought were not to be found in their home, adding that her husband did not normally take work home. As a result of the search, among other objects, a laptop was found and seized. The applicant's wife pointed out that both she and her husband used the laptop. A search report was drawn up, describing the conduct of the search and the items found and seized. According to the report, the laptop was placed in a numbered "security bag" (*turvakott*). In the "remarks" section of the report, the applicant's wife mentioned that she had read the report and had no comments. Both the applicant's lawyer and his wife signed the search report.

13. In parallel to the search in the applicant's home a search was also conducted of his office at his law firm. The applicant was present during the search. In response to the proposal to hand over the searched objects, the

applicant noted that his mobile telephone had already been seized and that all the electronic documents were in his computer which had been sent to maintenance. He stated that he did not wish to reveal the exact whereabouts of the computer as it contained information on criminal proceedings relating to his various clients. During the search the applicant telephoned his lawyer, who was present at the search taking place in the applicant's home. Nothing was seized from his office. The applicant signed the search report and stated that he did not have any remarks or comments about the conduct of the search.

14. On the afternoon of 13 February 2018 the applicant was questioned as a suspect. He stated that he had provided legal counselling to other suspects in the criminal case as well as to their respective companies as part of his professional activities. He also mentioned that the business activities relating to a specific company, S, in which he was a shareholder, did not concern his professional activities as a lawyer. He pointed out that his "home computer" would contain documents concerning that company S.

15. Between 13 and 19 February 2018 the PBGB copied the full content of the applicant's mobile telephone and the hard drive of his laptop on to an external hard drive (mirror-image copies). An examination report (*vaatlusprotokoll*), signed by two officers, was drawn up. According to the report the examiner had verified that the bags in which the items had been placed had not been previously opened. The copies were to be kept at the data storage facility of the PBGB. The mobile telephone was returned to the applicant on 14 February 2018 and the laptop on 23 February 2018.

16. On 14 February 2018 the PBGB asked the applicant's law firm to provide them with bills for the services that the law firm had provided to two suspects in the criminal case as well as to the companies related to them. On 27 March 2018 the law firm replied that they could confirm having concluded legal counselling contracts (*õigusabileping*) with the said persons, observing that the applicant was one of the persons providing legal services. Referring to the duty of confidentiality, they provided no further information on the services.

II. THE SUBSEQUENT DOMESTIC PROCEEDINGS

17. On 7 March 2018 the applicant lodged an application with the PBGB, explaining that the seized mobile telephone and laptop belonged to his law firm and were used for the provision of legal services. He asked the PBGB not to examine the mobile telephone and laptop, not to use material copied from them as evidence in the criminal proceedings and to delete all the data that might have been copied.

18. In its reply of 21 March 2018, the PBGB explained that the fact that the applicant had used his laptop for providing legal services as a lawyer as well as for business activities outside his profession as a lawyer did not

mean that the guarantees provided in section 43(3) of the Bar Association Act (*advokatuuriseadus*; see paragraph 38 below) covered the data carrier in its entirety. In doing so the applicant had knowingly created a situation whereby the data contained therein would be seized as a result of a search. The aim of the search of the applicant's home had not been to access and seize data relating to the applicant's professional activities as a lawyer, but to obtain information concerning his activities in company S. The PBGB added that the data on the laptop and mobile telephone had been copied and would be searched on the basis of keywords. Other files with no evidentiary value would not be accessed.

19. On 27 March 2018 the applicant lodged a complaint with the Office of the Prosecutor General. Referring to section 43(3) of the Bar Association Act he requested that the seizure and other procedural actions taken in relation to the mobile telephone and laptop be declared unlawful, and that any information obtained from these data carriers be not used in evidence in any criminal proceedings and be deleted.

20. On 26 April 2018 the State Prosecutor dismissed the complaint, noting that the search and seizure had been carried out in accordance with the Code of Criminal Procedure (*kriminaalmenetluse seadustik* – hereafter "the CCrP"). The search authorisations had covered not only the seizure of data carriers but also their subsequent examination. The State Prosecutor referred to section 5(4) of the Code of Ethics of the Bar Association, as well as to section 44(1)(4) of the Bar Association Act (separation of data carriers concerning the provision of legal services and preventing access to data carriers; see paragraphs 41-42 below). He added, referring to section 44(1)(1) of the Bar Association Act (see paragraph 40 below), that in the event that the data carriers contained information relevant to the lawyer's unlawful activities, they would not benefit from the inviolability guarantee of section 43(3) of the same act.

21. On 5 May 2018 the applicant lodged a further appeal referring to the absolute nature of the requirement set out in section 43(3) of the Bar Association Act regardless of whether the relevant data carriers included information unrelated to the provision of legal services, whether anyone else had had access to them or whether the lawyer had complied with section 44(1)(4) of the Bar Association Act. He added that he had provided legal services to company S as part of his professional activity as a lawyer. He noted also that the possible keywords could equally be found in documents that were not related to the criminal investigation. The applicant argued that the inviolability rule would lose all its meaning if its application depended on the prosecution's assumptions about whether or not the data carriers contained information referring to the lawyer's unlawful activities.

22. On 4 June 2018 the Chief State Prosecutor dismissed the appeal, referring, *inter alia*, to a decision of the Tallinn Court of Appeal to the effect that the inviolability of lawyer's data carriers was not absolute in

situations where the said lawyer had been directly involved in committing an offence (see paragraph 47 below). In the instant case the applicant had been declared a suspect. The decision also referred to the Supreme Court judgment in case 3-1-1-22-10 (see paragraph 48 below).

23. The applicant's further appeal was dismissed by the Harju County Court on 6 July 2018. The court disagreed that the inviolability of lawyers' data carriers was absolute, and noted that it applied only in so far that the lawyer did not commit an offence in the framework of providing legal services. The court also noted that it was reasonable to expect that a lawyer would systematise the information on his electronic data carriers so as to differentiate documents relating to one client from those relating to another. The court suggested that the lawyer whose data carriers were being examined in the proceedings could submit an application to attend such an examination. No appeal lay with the decision.

24. Between 19 and 26 July 2018 the content of the applicant's mobile telephone and laptop were examined on the basis of thirty keywords. An examination report (*vaatlusprotokoll*) was drawn up and signed by two officers. The keywords included the names of some of the other suspects, names of companies as well as more generic terms such as "financial year" (*majandusaasta*) and "credit line" (*krediidiliin*). A visual search was carried out of the applicant's SMS messages. The report notes that "e-mails, SMS messages, documents and photos" were printed out, and they have been numbered and annexed to the report. The copies of the files examined were to be kept at the PBGB data storage facility. The applicant had not asked to be present during the examination.

25. On 23 November 2018 the pre-trial proceedings were completed and the material in the criminal file was handed to the applicant for examination. He was given until 18 January 2019 to submit any requests (see paragraph 33 below). The applicant did not lodge any requests concerning the seizure of the laptop and mobile telephone or their subsequent examination.

26. The applicant was committed for trial on 7 February 2019 on charges of being a member of a criminal organisation and of using forged documents.

27. At the hearing in Harju County Court on 5 March 2019, the applicant's representative argued that the search and the subsequent examination of the applicant's data carriers had been unlawful and that the evidence thus obtained should not be admitted in the proceedings. The judge of the Harju County Court noted that challenging procedural acts by appealing against investigative activities – *uurimiskaebemenetlus* (see paragraphs 34-35 below) – did not prevent the accused from raising the question of admissibility of the evidence obtained via such measures at the trial stage of the proceedings and did not prevent the court from expressing its opinion on the matter.

28. At the hearing on 11 August 2020 the prosecutor submitted the examination report concerning the content of the applicant's laptop and mobile telephone as evidence (see paragraph 24 above). The applicant pointed out that although the information obtained by examining his data carriers was unlawful, he did not object to the court admitting it in evidence, stating that he considered it vindicatory. The applicant did not contest any of the keywords used for examination of the content of the data carriers.

29. At the time of receipt of the parties' observations, the applicant's criminal proceedings were still ongoing.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. RELEVANT DOMESTIC LEGISLATION

A. Code of Criminal Procedure

30. Article 83 of the Code of Criminal Procedure (CCrP) concerns the examination (*vaatlus*) of, *inter alia*, physical evidence. Article 83 § 3 provides that if an explanation from a suspect, an accused, a witness, a qualified person or a victim is considered conducive to ensuring the thoroughness, comprehensiveness and objectivity of the examination, that person may be asked to attend the examination.

31. Article 91 of the CCrP concerns searches.

Article 91 § 1 provides that the aim of the search is, *inter alia,* to find an object to be confiscated or used as physical evidence, a document, or an item or person necessary for elucidating a criminal offence. A search may be conducted where there is a reasonable suspicion that the object is to be found at the place of the search.

Article 91 § 2 provides that, unless otherwise provided in the CCrP, a search may be conducted at the request of the Prosecutor's Office, on the basis of an order issued by a preliminary investigation judge or on the basis of a court order (*eeluurimiskohtuniku määruse või kohtumääruse alusel*). Both a preliminary investigation judge's order and a court order may take the form of an endorsement added to the request submitted by the Prosecutor's Office (*võib olla koostatud pealdisena prokuratuuri taotlusel*).

Article 91 § 3 provides a reference to a list of offences with respect to which the search authorisation may be given by the Prosecutor's Office. This does not apply to searches conducted on the premises of a law firm (*advokaadibüroo*).

Article 91 § 4 provides that the search warrant (*läbiotsimismäärus*) must explain the object of the search, the reasons for the search and the place where the search is to be conducted.

Under Article 91 § 8 a law firm (*advokaadibüroo*) must be searched in the presence of the lawyer (*advokaat*) whose premises are being searched. If

the lawyer cannot be present during the search, the search must be conducted in the presence of another lawyer providing legal services through the same law office, or if this is impossible, another lawyer.

Article 91 § 10 provides that in the course of a search, all objects which are subject to confiscation or clearly constitute evidence in the criminal proceedings may be seized provided that they were discovered without any search in a clearly visible place or in the course of a reasonable search undertaken in order to find the requisite items.

32. Article 125 concerns the storage of physical evidence. Article 125 § 1 provides that physical evidence must be stored in a criminal file, in the physical evidence storage facility of an investigative body, at the prosecutor's office, at court or on other premises in its possession or jurisdiction, or in a forensic institution. Otherwise, the measures prescribed in Article 126 of the CCrP will be applied to the physical evidence unless that would prejudice the criminal proceedings in the case. Article 125 § 3 obliges the person with whom physical evidence is deposited to ensure the inviolability and preservation of the evidence.

33. Article 225 § 1 provides that participants in proceedings may submit requests to the Prosecutor's Office within ten days as of the date of submission of the criminal file to the participants for examination. Article 225 § 3 provides that the dismissal of such a request in pre-trial proceedings does not prevent its re-submission in the trial proceedings.

34. Under Article 228 § 1, a party to criminal proceedings has a right, before the relevant indictment is drawn up, to lodge an appeal with the Prosecutor's Office against a procedural action or an order issued by an investigating body if he or she considers that a violation of procedural requirements in the performance of a procedural action or in the preparation of an order resulted in his or her rights being violated (appeal against investigative activities, *uurimiskaebemenetlus*). Under Article 228 § 2, before the indictment is drawn up, the same person has a right to appeal to the Office of the Prosecutor General against an action or an order of the Prosecutor's Office.

35. Article 230 § 1 provides that if the activities of an investigating body or Prosecutor's Office violating a person's rights were contested, and the person did not agree with the decision of the Office of the Prosecutor General reviewing the appeal, the person has a right to lodge an appeal with the preliminary investigation judge of a county court.

B. Bar Association Act

36. Section 41(1)(3) provides that in the provision of legal services a lawyer can freely choose and use all available means and methods which are in conformity with law.

37. The first sentence of section 43(2) provides that information disclosed to a lawyer is confidential.

38. Section 43(3) provides that data carriers concerning the provision of legal services by a lawyer are inviolable.

39. Section 43(5) provides that a lawyer cannot be detained, searched or taken into custody on the basis of circumstances arising from his or her professional activities, unless so ordered by a county or city court. Nor can a law firm in which a lawyer provides legal services be searched on the basis of circumstances arising from his or her professional activities.

The commented edition of the Code of Conduct of the Estonian Bar Association explains, in relation to that provision, that a lawyer cannot generally be detained, searched or taken into custody. However, such actions may be permissible for serious public-interest reasons, such as when a lawyer has him or herself been involved in a criminal offence. Where such reasons exist, they must be validated by a court, and the detention, search or taking into custody may thus only be authorised by a court.

The commented edition of the Code of Conduct of the Estonian Bar Association also states that conducting searches in places other than a law office (such as in a lawyer's home or a car) can raise issues under criminal procedural law. On the one hand section 43(5) of the Bar Association Act provides that it should be authorised by a judge, but on the other hand Article 91 of the CCrP does not set out any such requirement. The authors suggest that, having regard to the primacy of the lawyers' professional guarantees, such searches should in any event be authorised by a judge. Similarly, searches of lawyers' homes or cars should take place in the presence of the lawyer concerned or another lawyer.

40. Under section 44(1)(1) a lawyer is required to use all available means and methods which are in conformity with law in the interests of a client, while preserving his or her professional honour and dignity.

41. Under section 44(1)(4) a lawyer must store data carriers concerning the provision of legal services separately from other data carriers in his or her possession.

C. Code of Conduct of the Estonian Bar Association

42. Article 5 § 4 of the Code of Conduct provides that a lawyer must ensure that no third person has access to his client's documents, correspondence or other information, or to any documents drafted by the lawyer in the course of rendering legal services to the client.

43. The commented edition of the Code of Conduct of the Estonian Bar Association provides further explanations on Article 5 § 4, pointing out that the obligation to keep confidential all the documents and data carriers that concern the provision of legal services corresponds to the obligation stipulated in section 44(1)(4) of the Bar Association Act. This principle

must be followed even if the clients' data is in the electronic format. That means that the material related to the clients' cases must be distinguished and separated from other files. The lawyer must be able to show that the clients' files are in a separate server. In a virtual server the separation derives from clearly marked catalogue structures.

D. Compensation for Damage Caused in Offence Proceedings Act

44. Section 7(1) of the Compensation for Damage caused in Offence Proceedings Act (*süüteomenetluses tekitatud kahju hüvitamise seadus*) provides that if the body responsible for conducting proceedings either negligently or knowingly violates the law that governs those proceedings and thereby causes damage to a person, that person has the right to demand compensation regardless of the final outcome of the offence proceedings whereby the damage was caused.

45. Under section 11(1) compensation for non-pecuniary damage is granted to a natural person under section 7 of the same Act only if, in the offence proceedings, that person was deprived of liberty, was tortured or treated in an inhuman or degrading manner, damage was caused to his or her health, or if the inviolability of his or her home or of private life was infringed, the confidentiality of his or her messages was violated or his or her honour or good name was defamed.

II. RELEVANT DOMESTIC CASE-LAW

A. Professional secrecy and the inviolability of data carriers concerning the provision of legal services

46. The Supreme Court's judgment of 10 June 2005 in case no. 3-3-1-30-05 concerned a lawyer's meeting with a client in prison. The case is relevant for the interpretation that the Supreme Court gave to section 43(5) of the Bar Association Act. The Supreme Court noted that section 43(5) of the Bar Association Act could not be interpreted as meaning that a search of an attorney in circumstances concerning his or her professional activity would, without exception, be unlawful in all cases without a county or city court order authorising the search. Prison administrations had to be able to prevent or combat an offence where a reasonable suspicion existed that a lawyer entering or exiting the prison was committing an offence or the lawyer's meeting with a prisoner was being used to commit an offence. In that case, the search of the lawyer was found to be unlawful since no such information (suspicion of an offence) existed.

47. In its judgment of 17 May 2010 in case no. 1-08-15079, the Tallinn Court of Appeal addressed the admissibility as evidence of electronic correspondence between the accused (not a lawyer) and a law firm. The

correspondence had been obtained from a search of one of the accused's cars and of a server used by a certain company. The court emphasised that the admissibility as evidence of such electronic correspondence should be analysed in the framework of the combined effect of the Bar Association Act and the CCrP. The court explained that Article 91 of the CCrP did not impose limitations on the use of data carriers seized in the course of a search. At the same time, section 43(2) of the Bar Association Act stipulated that information disclosed to a lawyer was confidential, and section 43(3) provided that carriers of data concerning the provision of legal services by a lawyer were inviolable. The court found that in a situation where a contractual relationship between a lawyer and a client existed and legal services were provided, and where the client had not of their own free will disclosed to third parties information relating to the provision of legal services, the protection of confidentiality extended to the electronic correspondence between a lawyer and a client found on the data carriers that had been seized during the search. The court furthermore agreed that the confidentiality could be breached in a situation where a lawyer had been directly involved in the commission of the offence. This was not so in the given case and the impugned correspondence was not admitted as evidence.

48. By judgment of 26 May 2010 in case no. 3-1-1-22-10, the Supreme Court addressed the question of the admission as evidence of correspondence between an accused and a lawyer that had been obtained by means of secret surveillance. Relying on a regulation then in force, the Supreme Court found that it did not permit accepting as evidence information provided by a lawyer in so far as it entailed matters that the lawyer had learned in the course of his or her professional activity. In the case in question it was found that a message and a telephone conversation between a lawyer and the accused had not concerned the provision of legal services. The court added that it was competent to assess whether certain information related to the provision of legal services and was thus governed by professional secrecy.

B. Challenging procedural measures during pre-trial and trial proceedings

49. By judgment of 13 May 2019 in case no 1-15-11032/308, the Supreme Court drew a distinction between such pre-trial measures that could be challenged only during the pre-trial proceedings (see paragraphs 34-35 above concerning appeal against investigative activities) and those that could (also) be challenged during the main proceedings. It noted that the measure in question – "obligation not to leave the place of residence" – was intended to guarantee the effectiveness of the proceedings and could only be challenged during the pre-trial stage of the proceedings. The court then went on to explain that the aim of the trial proceedings was

to elucidate whether the accused had committed an offence. In order to do so, it was necessary to examine and analyse various items of evidence, such as evidence which had been obtained by means of searches or secret surveillance. In other words, during the main proceedings questions concerning the admissibility of evidence had to be addressed and disputed.

C. Claims of non-pecuniary damage

50. By judgment of 13 June 2016 in case no. 3-1-1-34-16 the Supreme Court, relying on the Compensation for Damage Caused in Offence Proceedings Act (see paragraphs 44-45 above), upheld the judgment of the lower-instance court to compensate the plaintiff for the non-pecuniary damage caused by the unlawful surveillance activities in the criminal proceedings against him.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

51. The applicant, referring to legal professional privilege and the inviolability of data carriers that concern the provision of legal services, complained that the seizure of his laptop and mobile telephone and their subsequent examination had violated his rights as secured under Article 8 of the Convention.

Article 8 of the Convention reads as follows:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

A. Admissibility

1. The parties' submissions

(a) The Government

52. The Government, relying on several sub-arguments, held that the applicant had not exhausted domestic remedies.

53. Firstly, the Government underlined that as the applicant had failed to invoke legal professional privilege until almost a month after the seizure, he had failed to exhaust domestic remedies with respect to the procedural measures taken until 7 March 2018.

54. Secondly, the Government pointed out that the applicant had not asked to be present during the examination of the copied content of the laptop and mobile telephone, as suggested by the Harju County Court in its decision of 6 July 2018. In the Government's view, such a right derived from Article 83 of the CCrP (see paragraph 30 above).

55. Thirdly, the applicant had not made use of the possibility of submitting requests or complaints concerning the examination of the copied data, as provided in Article 225 of the CCrP (see paragraph 33 above). In the Government's view, the latter could not be regarded as a "duplicate remedy" to the one that the applicant had already used. It was only after being presented with the criminal file on 23 November 2018 that the applicant could have ascertained the extent of the examination of the copied data, including the keywords used, and have submitted his objections to that.

56. Fourthly, the Government noted that under procedural law the applicant could have contested the admissibility of the evidence which he considered to have been obtained unlawfully. The decision of the preliminary investigation judge of the Harju County Court had not been binding on the court hearing the main case (see paragraph 27 above). The Government stressed that the domestic courts' possible finding concerning the unlawfulness of evidence would inherently entail a finding concerning the legality of the collection of such evidence. However, the applicant did not challenge the admissibility of the evidence but rather considered that it spoke in his favour. Nonetheless, had he challenged the admissibility of the evidence and had the court found that the seizure of his laptop and mobile telephone and the examination of information extracted from them had been unlawful, the applicant would have been entitled to claim non-pecuniary damages under the Compensation for Damage Caused in Offence Proceedings Act (see paragraphs 44-45 above).

57. The Government also emphasised that the applicant had not specified at any time which information should have been considered as protected by lawyer-client confidentiality. Such a clarification would have been relevant, given that the applicant's laptop and mobile telephone were not seized from his office and were apparently not used solely for purposes of his work as a lawyer.

58. Finally, the Government submitted that the complaint was manifestly ill-founded.

(b) The applicant

59. The applicant had submitted his observations before the Harju County Court hearing of 11 August 2020 (see paragraph 28 above).

60. The applicant considered that he had exhausted the relevant domestic remedies before lodging his application with the Court.

61. Firstly, no appeal had lain with the Harju County Court's decision of 6 July 2018.

62. Secondly, there was no legal basis for the Harju County Court's suggestion, repeated by the Government, that the applicant could have asked to be present during the examination of the data extracted from his laptop and mobile telephone. Even if such a possibility had been granted under the law, it would not have prevented the breach of the applicant's rights, as by the time of the examination all the content of the laptop and mobile telephone had already been copied and there was nothing to prevent it from being examined by the authorities at any stage before or after the time when the applicant could have been present. The applicant considered that the only effective remedy after the seizure of the data carriers and the copying of their content would have been to renounce examining the copied data and to delete it.

63. Thirdly, the applicant disagreed that submitting "requests" under Article 225 of the CCrP (as opposed to lodging appeals under Article 228 of the CCrP) could be considered an effective remedy. He explained that in practice requests made under Article 225 of the CCrP often concerned proposals to terminate criminal proceedings or to settle the case through plea bargaining. This article was rarely used to challenge individual procedural acts. In any event, by the time the criminal file was presented to the applicant, the prosecutor's office had already twice dismissed his requests to refrain from examining the data extracted from the data carriers.

64. Fourthly, as regards challenging the admission of evidence during the trial proceedings, the applicant argued that in such a situation the domestic courts would only rule on the lawfulness of the evidence, not on the violation of his rights as a lawyer. He further considered that a prospect of a compensation award would not eliminate the violation of his rights under the Convention.

65. He added that under section 43(3) of the Bar Association Act he had no obligation to specify which particular files were covered by lawyer-client confidentiality, as under that provision the data carriers were protected in their entirety. In any event, expecting such a specification would be unreasonable in view of the large number of professional contacts held by the applicant, and would have led to the unlawful disclosure of his other clients who were not concerned by the ongoing criminal proceedings.

2. The Court's assessment

66. The Government has raised several preliminary objections concerning the exhaustion of domestic remedies.

67. The Court finds, firstly, that the applicant's failure to lodge the application with the PBGB immediately after the search cannot be seen as a failure to exhaust a domestic remedy. The applicant made use of the appeal against investigative activities provided in Articles 228 and 230 of the CCrP

(see paragraphs 34-35 above). It does not appear from domestic legislation, nor did the Government claim, that a corresponding application should have been lodged within a certain time-limit which the applicant had failed to respect. The relevant authorities, including the Harju County Court, had examined his complaint on the merits, rather than rejecting it as being submitted out of time.

68. Secondly, as to the possibility of asking to be present during the examination of the copied content of the applicant's mobile telephone and laptop, the Court agrees with the applicant. Despite the Harju County Court's suggestion that the applicant could lodge an application to that effect (see paragraph 23 above), there would appear to be no legal basis in domestic law that would grant an interested party a subjective right to be present during such an examination. The wording of Article 83 of the CCrP rather refers to the investigating authorities' discretion in that question. Moreover, the Government have not provided any examples of that provision indeed having been interpreted and applied so as to contain a subjective right to be present during the examination of the content of the data carriers. Thus, the mere possibility of lodging a request to that effect cannot be considered an effective remedy which the applicant is expected to exhaust. The Court further notes that the domestic law does not specify how the applicant's presence – even if granted – would have enabled him to prevent the authorities from interfering with his legal professional privilege. The Court will deal with this aspect in its examination of the merits of the case (see paragraph 107 below).

69. Thirdly, as to the right to submit requests to the prosecutor's office under Article 225 of the CCrP (see paragraph 33 above), the Court is not convinced by the Government's argument that this could be deemed an effective remedy. The Court reiterates that it is incumbent on the Government pleading non-exhaustion to satisfy it that the remedy was an effective one available in theory and in practice at the relevant time, that is to say that it was accessible, was capable of providing redress in respect of the applicant's complaints and offered reasonable prospects of success (see *Molla Sali v. Greece* (just satisfaction) [GC], no. 20452/14, § 89, 18 June 2020). In the case at hand, the Government have not explained what the practical consequences of the applicant's possible request under Article 225 of the CCrP could be. Nor has the Government presented any examples of the practical application of this alleged remedy, not least in the context of challenging the seizure of data carriers allegedly containing material covered by lawyer-client confidentiality. The Court has doubts as to whether in such circumstances the review by the prosecutor's office would meet the requisite standards of independence (compare *Avanesyan v. Russia*, no. 41152/06, § 32, 18 September 2014, and *Panteleyenko v. Ukraine*, no. 11901/02, § 80, 29 June 2006), and it is not clear whether a possible refusal by the prosecutor's office would be subject to a judicial

review. In any event, the Court observes that by the time the applicant could have made use of that alleged remedy, the keyword-based examination of the copied content of his mobile telephone and laptop had already been carried out (see paragraphs 24-25 above).

70. As to the Government's fourth non-exhaustion argument, the Court admits that under domestic law it might have been open to the applicant to raise his objections to the seizure and examination of his laptop and mobile telephone again in the main proceedings, where the emphasis would likely have been on the admissibility of that evidence. Even if this was to be seen as an effective remedy concerning the complaints under Article 8 of the Convention, the Court reiterates that in the event of there being a number of domestic remedies which an individual can pursue, that person is entitled to choose, for the purpose of fulfilling the requirement of exhaustion of domestic remedies, a remedy which addresses his or her essential grievance (see *Nicolae Virgiliu Tănase v. Romania* [GC], no. 41720/13, § 177, 25 June 2019). The applicant had already, in compliance with domestic law, unsuccessfully raised his complaints concerning lawyer-client confidentiality in the context of his appeal against the investigative activities, including before the Harju County Court. The Court stresses that the Government did not consider this to have been an ineffective domestic remedy. The Court has no reason to hold otherwise in the case at hand. In such circumstances, the Court finds that the fact that the applicant decided not to challenge the admissibility of the impugned evidence at the trial stage of the proceedings – even though he had argued that it had been obtained unlawfully –, but rather considered that it spoke in his favour, cannot be held against him when assessing whether he had exhausted domestic remedies in the context of the Convention proceedings.

71. As to the Government's argument that the applicant had not specified in the domestic proceedings exactly what information should have been covered by legal professional privilege, the Court agrees that that would indeed have been preferable in the circumstances, where lawyer-client confidentiality was being relied upon. However, the Government do not seem to have considered such clarification to be a self-standing remedy or a pre-requisite for using the remedy that the applicant exhausted. Moreover, given the domestic legal context (see paragraph 107 below), the Court cannot discern what the practical effects of such clarification would have been.

72. The Court accordingly concludes that the applicant has duly exhausted domestic remedies for the purposes of the admissibility of his complaint under Article 8 of the Convention. The Court further notes that the complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

(a) The applicant

73. The applicant noted that he was not challenging the lawfulness of the searches or of his detention. His complaint focused on the seizure of the data carriers.

74. In response to the Government's argument that there had been no interference with the applicant's rights under Article 8 (see paragraph 79 below), he explained that the fact that he had not immediately objected to the procedural acts during the search and seizure did not render the later examination of the data extracted from the data carriers lawful. What mattered was that by the time the PBGB had begun its examination of the copied data on 26 July 2018 they ought to have realised – following the proceedings brought by the applicant (see paragraphs 17-23 above) – that the information was covered by the inviolability rule.

75. The applicant stressed that the inviolability rule set out in section 43(3) of the Bar Association Act was unqualified. If the legislator had wanted to allow the investigative bodies, under some circumstances, to examine information on the data carriers covered by that section, it would certainly have provided for measures to protect information falling under legal professional privilege. The fact that the law did not entail such regulation only confirmed that the rule was absolute.

76. Even if a lawyer failed to keep the data carriers concerning the provision of legal services separate from other data carriers, it would not mean that all the data carriers in the lawyer's possession would cease to be covered by the inviolability rule. That claim by the Government had no legal basis and was not supported by case-law. In any event, that line of argument would mean that the investigative bodies could always seize data carriers, while indicating that – according to them – the lawyer had not fulfilled the separation requirement. Such a practice would be open to arbitrariness. It would also mean that data carriers lost their inviolability guarantee as soon as a lawyer, for example, used his mobile telephone to read the news or call a taxi. As such, the inviolability rule would lose all practical meaning. In any event, at no stage had it been argued that his mobile telephone had contained information unrelated to the provision of legal services.

77. The applicant further argued that the fact that his wife had also been using the laptop did not eliminate the inviolability guarantee. The Government's suggestion to that effect had no legal basis. Moreover, his wife was not a suspect in the proceedings, nor had she ever stored anything on the laptop.

78. As to the information stored on the laptop concerning company S, the applicant explained that in addition to being a shareholder in that company he had also provided company S with legal services as part of his professional activity. This meant that the inviolability guarantee still applied.

(b) The Government

79. The Government argued that the seizure of the applicant's laptop and mobile telephone had not interfered with his rights under Article 8 of the Convention, as the applicant himself had failed to invoke legal professional privilege during the impugned seizure and for approximately a month after that. The Government noted that the applicant had been able to have a telephone conversation with the lawyer who had been present during the search at the applicant's home. Moreover, the applicant had himself noted during the search of his office that the computer he used for work had been sent to maintenance. Under those circumstances, the authorities conducting the search had been under no obligation to treat the said data carriers as being covered by legal professional privilege. The Government held that in a situation where data carriers were seized outside a law office, a failure on the part of the person concerned to notify the authorities of the risk of breaching legal professional privilege carried significant weight.

80. The Government further explained that the seizure and subsequent examination of the content of the applicant's laptop and mobile telephone had had a legal basis. The domestic law was foreseeable and provided sufficient guarantees against arbitrariness (see paragraphs 31, 37, 39 above). It had been possible to contest the procedural acts at various stages in the proceedings.

81. The Government, referring to section 44(1)(1) of the Bar Association Act and the domestic case-law (see paragraphs 47-48 above), stated that the inviolability of the data carriers provided for in section 43(3) of that Act did not extend to circumstances where the lawyer himself was suspected of committing a criminal offence or where the information concerned was unrelated to the provision of legal services. The Government stressed that the primary aim of legal professional privilege was to protect the interests of lawyers' clients. The Government further noted that relying on legal professional privilege presupposed that the lawyer complied with the duties concerning separation of the data carriers and preventing any third-party access to professional information (see paragraphs 41-42 above).

82. In the instant case, the applicant was suspected of having committed a crime. His detention and the search of his home and vehicle had been duly authorised by a preliminary investigation judge. The request for the search had sufficiently detailed the premises to be searched as well as the items to be searched for. The fact that the preliminary investigation judge had given the authorisation for the search of the applicant's home and vehicles by way

of an endorsement (see paragraph 31 above) could not be regarded as meaning that there had been no substantive review by a court. Rather it meant that the judge had accepted the prosecutor's office's detailed request. The Government cited examples where the courts, also by way of an endorsement, had refused to authorise searches on the scale requested by the prosecutor's office. A lawyer of the applicant's choosing had been present during the search at his home. The search warrant was presented to the applicant's wife and his lawyer. The conduct of the search and the applicant's detention were documented, and the applicant and his lawyer had an opportunity (which they did not take) to record their objections in the relevant reports. The Government noted that a search, by nature, entailed the seizure of items such as data carriers.

83. Although the full content of the applicant's laptop and mobile telephone had been copied, that had been done in order to ensure the rights of the accused. Having a one-to-one mirror-image copy ensured the integrity of the data and helped to avoid any allegations of data manipulation by adding or erasing items. In any event, the subsequent examination of the data, carried out on the basis of thirty keywords, had remained within the boundaries of the authorisation of 12 February 2018. The Government emphasised that the aim had not been to seek material covered by lawyer-client confidentiality, but to retrieve information concerning offences committed by the applicant outside his professional activities as a lawyer. The Government also stressed that the applicant had not differentiated files concerning the provision of legal services from any other files on his laptop, nor had he indicated during the search and seizure or afterwards which files were subject to lawyer-client confidentiality.

2. The Court's assessment

(a) Preliminary remarks

84. The Court relies on the applicant's argument that he was not challenging the lawfulness of the searches as such or the lawfulness of his detention, but rather complaining about the seizure of his laptop and mobile telephone. Having regard to the content of the complaint raised in the application form lodged with the Court, the Court considers that the applicant's complaint also covers the examination of the said data carriers after their seizure by the police. In the analysis below, the applicant's detention and the search of his home and his car will be mentioned in so far as the disputed seizures took place in the context of the given procedural steps and were covered by the warrants of the preliminary investigation judge, dated 12 February 2018.

(b) Existence of an interference

85. In so far as the applicant complains about the seizure of his data carriers and their subsequent examination, the Court finds that those acts constituted an interference with his right to respect for his "correspondence". The failure of the applicant or his lawyer to invoke legal professional privilege immediately during the search (see the Government's argument in paragraph 79 above) does not alter that finding. The Court, moreover, notes that the fact that the applicant was a lawyer by profession was well known to the prosecutor's office. Indeed, the State Prosecutor noted in the application for a search of the applicant's home and vehicles that the search might bring to light information that related to the applicant's professional activities as a lawyer (see paragraph 9 above).

(c) Existence of legal basis and procedural safeguards in domestic law

86. As to the question of whether the measure was in accordance with the law, the Court's case-law has established that a measure must have some basis in domestic law, the term "law" being understood in its "substantive" rather than its "formal" sense. In a sphere covered by statutory law, the "law" is the enactment in force as the competent courts have interpreted it. Domestic law must further be compatible with the rule of law and accessible to the person concerned, and the person affected must be able to foresee the consequences of the domestic law for him or her (see *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, § 332, 25 May 2021; *Wolland v. Norway*, no. 39731/12, § 62, 17 May 2018; see also *Golovan v. Ukraine*, no. 41716/06, § 56, 5 July 2012).

87. In the context of searches and seizures, the domestic law must provide some protection to the individual against arbitrary interference with Article 8 rights. It must thus be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances and conditions under which public authorities are empowered to resort to any such measures (see *Golovan*, cited above, § 57).

88. Furthermore, the Court has acknowledged the importance of specific procedural guarantees when it comes to protecting the confidentiality of exchanges between lawyers and their clients (see *Saber v. Norway,* no. 459/18, § 51, 17 December 2020, and *Sommer v. Germany*, no. 73607/13, § 56, 27 April 2017; see also *Kadura and Smaliy v. Ukraine*, nos. 42753/14 and 43860/14, §§ 144-45, 21 January 2021).

89. The Convention does not prohibit the imposition on lawyers of certain obligations likely to concern their relationships with their clients. This is the case in particular where credible evidence is found of the participation of a lawyer in an offence, or in connection with efforts to combat certain practices. On that account, however, it is vital to provide a strict framework for such measures, since lawyers occupy a vital position in

the administration of justice and can, by virtue of their role as intermediary between litigants and the courts, be described as officers of the law (see *André and Another v. France*, no. 18603/03, § 42, 24 July 2008).

90. Turning to the present case, the Court accepts that the interference can be said to have had a general legal basis in domestic law, namely Article 91 of the CCrP.

91. The Court will further examine the "quality" of the legal rules applicable to the applicant in the instant case. In doing so, it will first address the question whether the domestic law is sufficiently clear as regards the (in)ability to rely on legal professional privilege in circumstances where a lawyer him or herself is suspected of having participated in an offence. Secondly, the Court will examine whether the domestic law provides requisite procedural guarantees for the protection of the confidentiality of exchanges between lawyers and their clients.

92. Turning to the first of the questions mentioned in the preceding paragraph, the Court notes that the applicant's key argument is that under section 43(3) of the Bar Association Act all lawyers' data carriers concerning the provision of legal services are inviolable in their entirety, and that such inviolability is absolute. The Government, however, argued that the inviolability rule did not apply when the lawyer him or herself was suspected of a criminal offence or when the relevant data did not concern the provision of legal services. They further argued that such inviolability, in its absolute terms, could not be relied on where the lawyer had failed to duly separate the information covered by legal professional privilege from other material not covered by such privilege.

93. The Court notes that it follows from the wording of section 43(3) of the Bar Association Act that it grants inviolability to data carriers only in so far as they are related to the provision of legal services. It will address the question of possible procedural guarantees under circumstances where the seized data carriers contain material covered by legal professional privilege and information unrelated to the provision of legal services below (see paragraphs 98-100 and 105-107 below).

94. The Court also observes that despite the seemingly unqualified wording of the inviolability rule laid down in section 43(3) of the Bar Association Act, the Government referred to other relevant provisions of domestic law and domestic case-law in support of their argument that the inviolability of lawyers' data carriers is not absolute (see paragraphs 39-42 and 47-48 above). The Court acknowledges that it is first and foremost for the domestic courts to interpret and apply domestic law. It therefore accepts that the domestic law provides some support for finding that the inviolability rule set out in section 43(3) of the Bar Association Act must yield where a lawyer him or herself is suspected of a criminal offence. In the Court's opinion it remains doubtful, however, whether the domestic law

– as it currently stands – can be said to meet the requirements of clarity and foreseeability, as required under its case-law.

95. Nevertheless, the Court does not find it necessary to adopt a definitive position on this matter, because, for the reasons set out below, it considers that the domestic law in any event does not provide sufficient procedural safeguards in order to prevent arbitrary or disproportionate interference with legal professional privilege.

96. Turning to the aspect of procedural safeguards, the Court notes that under domestic law there are certain safeguards in place relating to searches and seizures in general, as well as to the context of searching lawyers' premises. Indeed, under domestic law, a search may be carried out if there is a reasonable suspicion that the object is to be found on the premises to be searched. Furthermore, the search warrant must generally specify the object, place of and reasons for the search (see paragraph 31 above). In the event that a search is carried out at a law firm, it must be authorised by an order of a preliminary investigation judge or a court order and the search must be conducted in the presence of the lawyer whose premises are being searched or another lawyer (see paragraph 31 above).

97. The Court observes, however, that the CCrP does not appear to require the presence of the lawyer concerned (or another lawyer) in the event that the premises to be searched are not a law firm but a lawyer's home or a vehicle or seem to impose a requirement for judicial authorisation in such circumstances. It seems, nonetheless, that such requirements may arise under section 43(5) of the Bar Association Act (compare paragraphs 31 and 39 above). It also appears that the domestic law leaves it to the judge to decide whether or not to authorise the search by way of a fully reasoned order or an endorsement. Despite authorisations in the form of endorsement being logically more succinct, it does not seem that the choice of such a form would make it technically impossible or prevent the domestic judge from adding reasons or conditions of his or her own as an operative part of the decision to authorise the search.

98. Despite the safeguards referred to above, the Court's essential concern is the lack of a practical framework for the protection of legal professional privilege in cases such as the present one. Working on the premise that under domestic law professional legal privilege does not apply to the extent that the lawyer him or herself is a suspect and/or acted in a capacity other than a lawyer, the key question is how privileged material is distinguished and separated from material where the lawyer-client confidentiality cannot be relied on. The Court notes that it was not established in the domestic proceedings and that it clearly does not follow from the Government's observations that under domestic law lawyer-client confidentiality stops applying altogether with respect to a lawyer who is a suspect in a criminal case, or who also engages in activities other than

providing legal services and/or fails to duly separate various privileged and non-privileged material.

99. 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.

100. 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. In that regard, the Court is prepared to accept the Government's argument that making a mirror-image copy can been seen as a procedural guarantee against any possible manipulation of the content of those data carriers (see *Wolland*, cited above, § 76; compare and contrast *Iliya Stefanov v. Bulgaria*, no. 65755/01, § 42, 22 May 2008, and *Kolesnichenko v. Russia*, no. 19856/04, § 43, 9 April 2009). Such a practice would, moreover, allow the authorities to return the seized data carriers relatively promptly to their owners and – should the owners be lawyers or law firms – avoid their work from being unduly inhibited for longer than is absolutely necessary.

101. The Court emphasises that the lawyer's obligation under the domestic law (see paragraphs 41-43 above) to separate data carriers used in the provision of legal services and the obligation to use clearly marked catalogue structures for clients' files – if properly followed – would contribute considerably to carrying out the sifting task.

102. The Court draws attention to the fact that in addition to safeguards addressing the seizure of data carriers and/or copying of their content as well as the sifting of digitally stored data, it is also important to prevent unwarranted and unrecorded access to the data carriers and/or processing of the data from the moment that it is seized until it is either returned or destroyed in due course.

103. Turning to the circumstances of the instant case, the Court observes that the domestic law does not seem to contain any specific procedure or safeguards to address the examination of electronic data carriers and prevent communication covered by legal professional privilege from being compromised. The Court considers that this lack of a practical procedural scheme and safeguards is, to a lesser or greater extent, also reflected in how, in the instant case, the search was authorised and how the subsequent copying of the seized data carriers and the examination of their content was carried out.

104. In the case of the applicant, the search warrant issued by the preliminary investigation judge made no provision for safeguarding the possible privileged material protected by professional secrecy (compare *Kruglov and Others v. Russia*, nos. 11264/04 and 15 others, §§ 128-29, 4 February 2020; *Iliya Stefanov*, cited above, § 41; and *Smirnov v. Russia*, no. 71362/01, § 46, 7 June 2007). This was the situation despite the fact that the State Prosecutor's application for a search warrant had specifically included reference to the possibility that the applicant might be in possession of information related to his professional activities as a lawyer but that would not be of relevance in the context of the ongoing criminal proceedings (see paragraph 9 above).

105. Although the applicant was later assured that the search of the content of his laptop and mobile telephone would take place on the basis of keywords – and such a search was indeed carried out – this obligation did not seem to derive from domestic legislation. Accordingly, the keyword-based search was not envisaged in the State Prosecutor's application for authorisation of a search, nor was such an obligation mentioned by the preliminary investigation judge in the search warrants (compare *Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal*, no. 27013/10, 3 September 2015).

106. Rather, it appears that the decision of whether to conduct a keyword-based search (or use any other method of sifting) as well as the choice of relevant keywords was left entirely up to the investigative authorities. At this juncture, the Court observes that some of the keywords used for the search (such as "financial year" or "credit line") were notably broad in scope. The Court has already found above that the domestic law did not grant the applicant any right to be present during the keyword-based search (see paragraph 68 above).

107. In any event, it remains unclear from the domestic law how any potential disputes between the investigative authorities and the lawyer concerned over the keywords to be used or any other methods of filtering the electronic content would be resolved. Indeed, the domestic law does not seem to have any specific rules about the procedure to be followed in the event that either the lawyer or his representative objects to the seizure or content examination with reference to lawyer-client confidentiality (compare, for example, *Robathin v. Austria*, no. 30457/06, § 50, 3 July 2012; *Wieser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, §§ 60 and 62, ECHR 2007-IV; and *André and Another*, cited above, § 44). The Court notes that the domestic law provides for the possibility to lodge an appeal against investigative activities. However, it does not appear to follow from the domestic law that material in respect of which the applicability of legal professional privilege is disputed would not be made available to the investigative authorities before the domestic courts have had a chance to conduct a specific and detailed analysis of the matter, and – if

necessary – order the return or destruction of seized data carriers and/or their copied content (compare *Kırdök and Others v. Turkey*, no. 14704/12, § 51, 3 December 2019; *Vinci Construction and GTM Génie Civil et Services v. France*, nos. 63629/10 and 60567/10, § 79, 2 April 2015).

108. Against the background of a scarce legislative framework, the Court finds that the practical relevance as a safeguard of the presence of the lawyer concerned or another lawyer during the search – or even during the actual examination of the copied content of data carriers – is of limited effect.

109. Although the domestic legislation lacked the appropriate procedural safeguards in order to protect data covered by legal professional privilege, the Court has no basis on which to decide whether or not lawyer-client confidentiality was actually compromised in the case at hand. In the Court's view, however, the lack of procedural guarantees relating specifically to the protection of legal professional privilege already fell short of the requirements flowing from the criterion that the interference must be in accordance with the law within the meaning of Article 8 § 2 of the Convention (see *Saber*, cited above, § 57). Having drawn that conclusion, it is not necessary for the Court to review compliance with the other requirements under that provision.

110. In the light of the above, the Court finds that there has been a violation of Article 8 of the Convention.

II. APPLICATION OF ARTICLE 41 OF THE CONVENTION

111. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

112. The applicant, referring to the professional and personal consequence of the seizure and examination of the data carriers, claimed 12,000 euros (EUR) in respect of non-pecuniary damage. He did not submit a claim in respect of pecuniary damage.

113. The Government, referring to the arguments raised with regard to the admissibility of the application, considered that account should be taken of the applicant's own behaviour during the search and seizure, and that the finding of a violation therefore would, in itself, constitute sufficient just satisfaction.

114. The Court, in view of the circumstances of the case and the nature of the violation found, considers that it is not necessary to award just satisfaction.

B. Costs and expenses

115. The applicant made no claim as regards the costs and expenses incurred before the domestic courts or for those incurred before the Court.

116. The Court will, accordingly, not award the applicant any compensation under this head.

FOR THESE REASONS, THE COURT,

1. *Declares*, by a majority, the application admissible;

2. *Holds*, by four votes to three, that there has been a violation of Article 8 of the Convention;

3. *Holds*, unanimously, that it is not necessary to award just satisfaction.

Done in English, and notified in writing on 16 November 2021, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

{signature_p_2}

Milan Blaško
Registrar

Georges Ravarani
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

(a) Concurring opinion of Judge Pavli;
(b) Joint dissenting opinion of Judges Ravarani, Seibert-Fohr and Zünd.

G.R.
M.B.

CONCURRING OPINION OF JUDGE PAVLI

1. I am in full agreement with the outcome and reasoning of today's judgment. I am writing separately in order to emphasise two sets of issues that I consider to be of great importance for the fate of lawyer-client privilege, a cornerstone of defence rights, in our digital age.

2. The first point relates to the question of what constitutes an interference with said privilege and whether a practising lawyer should be required to prove that some form of "actual harm" followed from searches and seizures of privileged materials and communications. Any such requirements are based, in my view, on a conception of legal professional privilege that would be alien to most practising lawyers. It is also a conception that stands at odds with the Court's well-established jurisprudence on the protection of personal and/or otherwise protected data: any capture of such data by a public authority is in principle sufficient to constitute an *interference* with the relevant interest protected by the Convention. This approach was confirmed recently by the Grand Chamber, in the bulk surveillance context, in *Big Brother Watch and Others v. the United Kingdom* (nos. 58170/13 and 2 others, § 330, 25 May 2021), both generally and with respect to the comparable privilege enjoyed by the press in relation to confidential journalistic material (ibid., §§ 447-50).

3. In other words, there is a presumption that any seizure of prima facie privileged data by the authorities is capable of undermining the confidentiality of the material unless strict data-searching safeguards are in place, usually involving some form of judicial review. The burden is on the authorities to show that they have not unduly interfered with the privilege. Any other approach to the question of victim status would turn this presumption on its head. After all, the applicant is a criminal defence lawyer and at least some of his clients – that is to say, those who were not connected in any way with the investigation in which the applicant himself was a suspect – were potentially under investigation by the same police department that had seized his electronic devices. I would think that would be enough to make most defence lawyers, as well as their clients, quite nervous.

4. Secondly, the respondent Government have argued, in effect, that LPP protection depends on a strict separation of privileged material from other, non-protected, data (see paragraph 81 of the judgment). While this is certainly a proper ethical standard to be followed by defence lawyers, the claim that the current applicant failed to do so is based on assumptions that are not univocally supported by the record before us.

5. Furthermore, historical notions about the neat separation of privileged and non-privileged material may need to be recalibrated for our digital ways and mores. For example, how many of us can claim to keep an impenetrable wall between the personal and professional data held within our

smartphones? Perhaps practising lawyers should be held to a higher standard – but what applies to paper records may not apply as easily to our increasingly complex digital lives. Practices and ethical standards in this field are still evolving. Finally, even assuming that a defence lawyer has been somewhat lax in the handling of privileged material, that should not give police departments *carte blanche* to undertake fishing expeditions through his or her data – whose confidentiality, it should be recalled, is guaranteed in the first place for the benefit of the lawyer's clients.

6. I have little doubt that the challenges of protecting sensitive electronic data will continue to keep the Court occupied in the coming years. I also believe that the current judgment's emphasis on the need for rigorous legislative frameworks in this field, including with respect to search modalities and other digital-specific arrangements, is the correct approach. We need to adapt fundamental protections to the realities of the digital age, without losing sight of their *raison d'être*.

JOINT DISSENTING OPINION OF JUDGES RAVARANI, SEIBERT-FOHR AND ZÜND

1. Though we share the majority's general concerns about the insufficient clarity and foreseeability of the legislative framework in respect of the seizure of data protected by legal professional privilege (LPP), with regret we cannot agree with the majority's finding that the application was admissible, as we consider that the applicant could not claim to be a victim of a violation of Article 8 of the Convention.

2. The starting point is section 44(1)(4) of the Bar Association Act (see paragraph 41 of the judgment; see also the commented edition of the Code of Conduct of the Estonian Bar, mentioned in paragraph 43), which requires that a lawyer "must store data carriers concerning the provision of legal services separately from other data carriers in his or her possession".

3. The reason behind this provision is quite obvious and has to be seen in the context of legal professional privilege (LPP), which is aimed at protecting the confidentiality of exchanges between lawyers and their clients and which is a cornerstone of the right of defence in a trial (see *Apostu v. Romania*, no. 22765/12, § 96, 3 February 2015, and *Altay v. Turkey (no. 2)*, no. 11236/09, § 50, 9 April 2019). Professional secrecy is the basis of the relationship of trust existing between a lawyer and his client (see *Saber v. Norway,* no. 459/18, § 51, 17 December 2020). Furthermore, the safeguarding of professional secrecy is, in particular, the corollary of the right of a lawyer's client not to incriminate himself (see *André and Another v. France*, no. 18603/03, § 41, 24 July 2008). The first sentence of section 43(2) of the Estonian Bar Association Act provides that information disclosed to a lawyer is confidential.

4. As LPP is aimed at protecting the confidentiality of exchanges between the lawyer and his or her clients, in principle the lawyer is not entitled to unilaterally waive the privilege and reveal the content of what he or she shares in confidence with the client. At the same time it is in the nature of LPP that the only data which benefit from such privilege are those that are shared by the lawyer and his or her client, as it is not designed to protect exclusively the lawyer but also, and even primarily, the client.

5. Section 44(1)(4) of the Bar Association Act seeks to delineate the scope of the information specially protected by LPP without conferring on the lawyer a discretion to have all data he or she stores protected without distinction, whatever their content. Its effectiveness therefore depends on scrupulous compliance, by the lawyer, with the obligation to store confidential information separately. Negligence or even deliberately wrongful behaviour in this regard will ultimately weaken the lawyer's and the clients' protection.

6. A problem arises if – as happened in the present case – the lawyer does not comply with this obligation and mixes the protected data with

unprotected data, for instance if he engages in other business. It is true that the clients should in no way suffer from such negligence or deliberately wrongful behaviour, but such protection should not lead to a situation where the lawyer him or herself can claim extended protection covering not only LPP information but also other data. He or she should not be entitled to claim protection of a privacy the limits of which he or she has blurred and which is mainly designed to protect somebody else, namely the client. In other words, should the applicant benefit from wrongful behaviour which he himself committed? The principle *nemo auditur turpitudinem suam allegans* (for an application of the principle by the Court, see *Monory v. Hungary and Romania* (dec.), no. 71099/01, 17 Feb. 2004) could easily be applied in such a context.

7. The judgment to some extent acknowledges the problem (see paragraph 101) but does not draw any inferences from it.

8. The fact that the applicant did not take advantage of the opportunity to be present during the examination of the seized data, as indicated by the judge (see paragraph 24 of the judgment), was certainly not very helpful. It is perhaps true that no such right was expressly enshrined in a legal provision, but the applicant could at least have discussed the relevance of the keywords with the investigators. Instead he showed a kind of disinterest in what was actually and concretely happening to the seized data.

9. The same is true of his choice not to submit any requests before the official investigation was closed (see paragraph 25 of the judgment), despite the fact that Article 225 § 1 of the Code of Criminal Procedure conferred such a right on him. It is of little relevance in this connection that the provision in question is apparently rarely used in that context and that the applicant had twice previously challenged the seizure of his laptop without success. As a matter of fact, had he been really interested in having the stored data protected he could have shown some diligence in this regard too.

10. Moreover, the applicant obviously did not suffer harm as a result of the violation of LPP. He did not even try to explain in what concrete sense he had suffered on account of the seizure of the data. It is true that his clients may have suffered harm as a result of the seizure, but this appears to be merely a hypothetical assumption in the absence of any concrete evidence submitted to the Court. We are unable to accept that LPP is an absolute right, failure to respect which entails a violation of Article 8 irrespective of the consequences of that failure. The applicant had a duty to show how and to what extent his rights and interests had been prejudiced. However, what he in fact did was to eventually rely expressly on the information drawn from the seized and copied data. His behaviour showed that he was not interested in the actual protection of the data but was ready to use the evidence allegedly found in violation of LPP for his own purposes, irrespective of the protection of his clients. In any event, the fact

that he actually relied on the data contradicts his assertion that he was negatively affected by their seizure.

11. These various elements lead us to the conclusion that the seizure of the data did not affect the applicant in the exercise of his rights under Article 8.