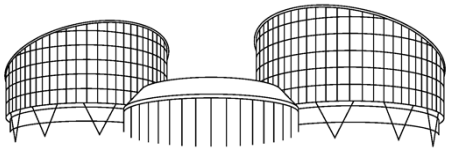

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIFTH SECTION

CASE OF SABER v. NORWAY

(Application no. 459/18)

JUDGMENT

Art 8 • Respect for correspondence • Insufficient legal framework and safeguards for protecting data subject to legal professional privilege during police seizure of smart phone and search of its mirror image copy

STRASBOURG

17 December 2020

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Saber v. Norway,

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

Síofra O'Leary, *President,*
Mārtiņš Mits,
Ganna Yudkivska,
Stéphanie Mourou-Vikström,
Ivana Jelić,
Arnfinn Bårdsen,
Mattias Guyomar, *judges,*
and Victor Soloveytchik, *Section Registrar,*

Having regard to:

the application against the Kingdom of Norway lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Norwegian national, Mr Mohammed Imran Saber ("the applicant"), on 27 December 2017;

the decision to give notice to the Norwegian Government ("the Government") of the complaints concerning Articles 6 and 8 of the Convention;

the parties' observations;

Having deliberated in private on 10 November 2020,

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

INTRODUCTION

1. The application concerns the applicant's complaint that proceedings in respect of search and seizure of data from his smart phone, facilitating access to correspondence between him and his lawyers, entailed a violation of Articles 6 and 8 of the Convention.

THE FACTS

2. The applicant, Mr Mohammed Imran Saber, is a Norwegian national who was born in 1978 and lives in Oslo. He was represented before the Court by Mr J.C. Elden, a lawyer practising in Oslo.

3. The Government were represented by their Agent, Ms H. Busch at the Attorney General's Office (Civil Matters), assisted by Ms L. Tvedt, an associate at the same office.

The circumstances of the case

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

5. In connection with an investigation into a criminal case against two persons for, among other things, conspiracy to murder the applicant – who, being a possible victim of an alleged crime, was accordingly an "aggrieved party" (*fornærmet*) in the sense that that term is employed in the domestic criminal procedural law – the applicant's smart phone was seized by the police on 23 November 2015. A mirror-image copy of the phone was captured, as the police wished to search it in order to shed light on possible conflicts between the suspects and the applicant. The phone was returned to the applicant. When the phone had been taken, the applicant stated that it contained his correspondence with two lawyers defending him (*forsvarsadvokater*) in another criminal case, in which he was a suspect.

6. Since the applicant had given information to the effect that the phone contained communications between the applicant and his lawyers, there were reasons to believe that some of the content of the mirror image copy would be exempt from seizure under Articles 204 and 119 of the Code of Criminal Procedure (see paragraph 29 below). On 4 January 2016 the prosecuting authority therefore decided to submit the mirror image copy to the Oslo City Court (*tingrett*) under the procedure set out in the last paragraph of Article 205, which the authority assumed applied by analogy. The prosecuting authority requested that the City Court peruse the mirror image copy and decide which parts of the data on it were subject to legal professional privilege (LPP) and which parts could be given to the police to search. At the same time the prosecuting authority declared that they had waived the seizure of those parts of the material that contained correspondence with the two above defence counsel or with the other counsel who assisted the applicant in his role as an aggrieved party in the case concerning conspiracy to murder (*bistandsadvokat*).

7. In the course of the continued proceedings before the City Court, the views of the parties were obtained. The prosecuting authority, counsel for the applicant in respect of his role as an aggrieved party, as well as defence counsel for the suspects in the case relating to conspiracy to murder, were given the opportunity to file submissions. Counsel for the applicant as an aggrieved party stated that the mirror image copy also contained confidential correspondence with other lawyers.

8. In a letter of 5 April 2016 the Oslo City Court listed the keywords that it proposed using in its perusal of the mirror image copy, in order to sift out data subject to LPP. The City Court suggested at the same time that it be assisted by a technical expert from the Oslo police. It was emphasised that the technical expert should not be associated with the investigation and was to sign a declaration of confidentiality.

9. In her reply of 9 April 2016, counsel for the applicant as an aggrieved party stated that she disagreed. She requested that a formal decision be given as to how to proceed with the search on the data on the mirror image copy. In addition, she argued that particular limitations to the prosecuting

authority's right to seize data applied when that data belonged to witnesses (which was the formal status of the applicant in the case relating to conspiracy to murder) and not to the persons charged.

10. In a letter of 8 August 2016 the Oslo City Court stated that the court would therefore not be assisted by an Oslo police technician in perusing the mirror image copy. The City Court would instead engage external technical assistance.

11. By letters of 30 August and 2 September 2016, the prosecuting authority objected to the engagement of external assistance by the City Court, as they feared that it could lead to the destruction of evidence. By letter of 29 September 2016, counsel for the applicant as an aggrieved party submitted that an attempt by the City Court to seek assistance from police officers in perusing the mirror image copy would breach Article 8 of the Convention.

12. By letter of 20 January 2017 to the Oslo City Court, the prosecuting authority made reference to a Supreme Court (*Høyesterett*) decision rendered – in an unrelated case – four days earlier; on 16 January 2017 (see paragraphs 30-40 below). Based on the decision, the prosecuting authority requested the return of the mirror image copy so that they could themselves examine it in order to assess which parts would be exempt from seizure. By letter of 10 February 2017, counsel for the applicant as an aggrieved party objected to the procedure proposed by the prosecuting authority, considering that it was for the City Court to examine the mirror image copy and filter out the data that should be exempt from seizure on account of LPP.

13. On 6 March 2017 the Oslo City Court declined jurisdiction for examining the mirror image copy in order to assess which data should not be subject to seizure. The City Court gave decisive weight to the Supreme Court's decision of 16 January 2017, and found that that decision prescribed that it was for the police to carry out that kind of filtering. It accordingly returned the mirror image copy to the police for examination and assessment of whether the different data on it could be seized in accordance with Articles 203 et seq. of the Code of Criminal Procedure (see paragraph 29 below).

14. The applicant appealed to the Borgarting High Court (*lagmannsrett*) against the City Court's decision. He also sought a stay of execution of the City Court's decision pending the outcome of the appeal. The latter request was turned down by the City Court.

15. In its decision of 12 June 2017, the High Court initially noted that the case concerned the procedure for perusing a data carrier that had already been seized by the police. Specifically, the prosecuting authority had, by analogy with the third paragraph of Article 205 of the Code of Criminal Procedure (see paragraph 29 below), requested that an examination be carried out by the City Court in order to filter out the data which were

subject to LPP and therefore exempt from seizure (which meant that the police would also not be entitled to search the data, then possibly deciding on their seizure); it was not a case in which seizure had been decided and the applicant subsequently requested that it be lifted pursuant to Article 208 (ibid.).

16. The applicant had principally argued that he, by virtue of the letters initially sent from the Oslo City Court in which that court had proceeded on the grounds that it was competent to peruse the mirror image copy with the assistance of an external technician, had a vested right to have that procedure followed. The High Court concluded on this point that the City Court had not taken any decisions to the effect that the applicant had acquired any rights relating to the procedure. It was therefore incumbent on the High Court to decide on the correct procedure.

17. Turning to this question of the correct procedure, the High Court took as its starting point the first section of Article 204 of the Code of Criminal Procedure, according to which documents about whose contents a witness would be entitled to refuse to testify were exempt from seizure (see paragraph 29 below). According to Article 119 a court was not entitled to take statements from lawyers about matters that had been vouchsafed to them in their capacity as lawyers. The High Court observed that conversations and messages between lawyers and clients enjoyed solid protection under the Code of Criminal Procedure and Article 8 of the Convention.

18. The High Court went on to examine the relevant Supreme Court case-law, in particular the Supreme Court's decisions of 27 March 2013 (published in *Norsk Retstidende* (*Rt*) 2013-968); 11 October 2013 (Rt-2013-1282); 27 January 2015 (Rt-2015-81); and 16 January 2017 (see paragraphs 30-40 below).

19. The instant case, the High Court observed, did not concern seizure of documents at a lawyer's office or a lawyer's premises. It was likely, however, that the mirror image copy comprised occasional communications between the applicant and his lawyers. There was still no information on whether such communications formed any sizeable part of the total data content of the copy.

20. According to the High Court, it was the prosecuting authority that had the primary competence to take decisions on seizure, as well as the primary responsibility for ensuring that seizures were not decided in respect of data that were exempt from seizure under the Code of Criminal Procedure. It observed that in its decision of 16 January 2017 the Supreme Court had carried out a thorough examination of the relevant legal sources, including the case-law of this Court with regard to Article 8 of the Convention.

21. In the High Court's view the City Court had rightly concluded that the prosecuting authority had the competence to peruse the data on the

mirror image copy. When carrying out such examination, the prosecuting authority would have to sift out any data that could be exempt from seizure. Any such data would, without any further inspection, have to be returned to the applicant or deleted. Data in respect of which the question whether they might be exempt from seizure could be raised would have to be transmitted uninspected to the City Court so that that court could peruse them pursuant to the application by analogy of the third paragraph of Article 205 of the Code of Criminal Procedure (see paragraph 29 below).

22. Moreover, the High Court observed that the exemption from seizure under Articles 204 and 119 of the Code of Criminal Procedure (see paragraph 29 below) was absolute; it applied regardless of the owner of the object in question. Accordingly, the fact that the smart phone in the instant case belonged to the aggrieved party and not, for instance, to an accused, could not lead to any other conclusion than that which followed from the Supreme Court's decision of 16 January 2017 (see paragraphs 30-40 below).

23. Lastly, the High Court noted that the City Court's decision of 6 March 2017 (see paragraph 13 above) had been based on the prosecuting authority's initial transmission of the mirror image copy to the City Court to enable the latter to peruse the data on it. In so doing the City Court had not taken any decision on items possibly to be seized or on details concerning the examination of such items. Such questions therefore fell outside the ambit of the appeal proceedings. The High Court nonetheless remarked that it had not been shown that the perusal could only be effected by searching for particular keywords. A keyword search would, however, have to be carried out in order to reveal which data were exempt from seizure. Reference was made to the Supreme Court's decision of 16 January 2017, with further reference to, *inter alia*, the decision reported in Rt-2015-81 (see paragraphs 30-40 below).

24. Relying on the above considerations, the High Court unanimously rejected the appeal.

25. On 25 June 2017 the applicant appealed to the Supreme Court against the High Court's decision. He also applied for the implementation of the High Court's decision to be suspended pending the outcome of the appeal. The latter request was turned down by the City Court.

26. On 30 June 2017 the Supreme Court's Appeals Leave Committee (*Høyesteretts ankeutvalg*), in a summary decision, unanimously concluded that the appeal against the High Court's decision clearly had no prospects of success and therefore rejected it.

27. The mirror image copy was thereafter returned to the police for search. This search was then carried out by the police themselves, without any control by the regional court at this stage. The procedure was described in a report from police officer E.S.R. of 9 November 2017. The report stated, *inter alia*, the following:

> "The seizure has been the subject of court proceedings, as Saber [(the applicant)] claimed that there are data items exempt from seizure on the phone, including legal correspondence with his defence counsel, attorney [Ø.S.] and attorney [P.D.]. Furthermore, attorney [S.E.] was appointed as counsel for Saber as aggrieved party on 30 September 2015 and it has also emerged that there is correspondence with her on Saber's phone.
>
> On the basis of decisions from the court, it has been decided, in consultation with [L.P.], who is responsible for the prosecution (*påtaleansvarlig*), that correspondence with the above-mentioned attorneys and lawyer's offices shall be removed from the mirror image copy which is to be examined by the police. It has also been decided that if the examination reveals contact that has not been captured (*fanget opp*), this shall not be examined."

The report stated, moreover, that the work with filtering out correspondence had been carried out by police officer A.K. at the Section of Digital Policework (*Seksjon for digitalt politiarbeid*) and specified the methods she had employed for that purpose.

28. The parties have not informed the Court of any further proceedings involving the data on the applicant's smart phone or of the further proceedings in respect of the case in which the applicant was the aggrieved party. The criminal proceedings against the applicant ended with his acquittal on 11 March 2019.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

A. The Code of Criminal Procedure

29. The 1981 Code of Criminal Procedure (*straffeprosessloven*), as in force at the relevant time, included the following provisions:

Article 119

> "Without the consent of the person entitled to the preservation of secrecy, the court may not receive any statement from clergymen in the state church, priests or pastors in registered religious communities, lawyers, defence counsel in criminal cases, conciliators in matrimonial cases, medical practitioners, psychologists, chemists, midwives or nurses about anything that has been confided to them in their official capacity. ...
>
> This prohibition no longer applies if the statement is needed to prevent an innocent person from being punished. ..."

Article 203

> "Objects that are deemed to be significant as evidence may be seized until a legally enforceable judgment takes effect. The same applies to objects that are deemed to be liable to confiscation or to a claim for surrender by an aggrieved person. ..."

Article 204

"Documents or any other items whose contents a witness may refuse to testify about under Articles 117 to 121 and 124 to 125, and which are in the possession either of a person who can refuse to testify or of a person who has a legal interest in keeping them secret, cannot be seized. In so far as a duty to testify may be imposed in certain cases under the said provisions, a corresponding power to order a seizure shall apply.

The prohibition in the first paragraph does not apply to documents or any other items that contain confidences between persons who are suspected of being accomplices to the criminal act [in question]. Nor does it prevent documents or any other items being removed from an unlawful possessor to enable them to be given to the person entitled thereto."

Article 205

"A decision relating to the seizure of an object that the possessor will not surrender voluntarily may be taken by the prosecuting authority. The decision shall as far as possible be in writing and specify the nature of the case, the purpose of the seizure, and what it shall include. An oral decision shall as soon as possible be rendered in writing. The provisions of Article 200, first paragraph, shall apply correspondingly.

When the prosecuting authority finds that there are special grounds for doing so, it may bring the question of seizure before a court. The provisions of the second to the fourth sentences of the first paragraph of this Article and of Article 209 shall apply correspondingly to the court's decision relating to seizure. The provisions of the first and third paragraphs of Article 208 shall also apply when seizure has been decided on by the court pursuant to this paragraph.

Documents or any other item in respect of which the possessor is not obliged to testify except by special court order may not be seized without a court order unless such a special order has already been made. If the police wish to submit documents to the court for a decision as to whether they may be seized, the said documents shall be sealed in a closed envelope in the presence of a representative of the possessor."

Article 208

"Any person who is affected by a seizure may immediately or subsequently demand that the question of whether it should be maintained be brought before a court. The prosecuting authority shall ensure that any such person shall be informed of this right.

The provision of the first sentence of the first paragraph shall apply correspondingly when any person who has voluntarily surrendered any object for seizure demands that it be returned.

The decision of the court shall be made by an order."

B. The Supreme Court's decision of 16 January 2017

30. In its decision of 16 January 2017, the Supreme Court considered the procedures governing the search of an extensive collection of e-mails collected from an accused person. After deciding on the specific case before it, the Supreme Court proceeded to attempt a general clarification of how, in procedural terms, to deal with situations where the police were examining

seized data, only to discover that they included correspondence with lawyers.

31. The Supreme Court stated that counsel in the case before it had argued that if the police, when perusing data items, came across correspondence with lawyers, the perusal would have to cease immediately and all items on the data carriers in question would have to be transmitted to the City Court so that that court could separate the data which were exempt from seizure from those which could be searched by the prosecuting authority and possibly seized, should they be found to contain evidence of interest. Counsel had further submitted that the latter procedure would also have to be followed where the accused person claimed that the materials collected included data that were exempt from seizure.

32. The Supreme Court disagreed with counsel's submissions. In the Supreme Court's view, one could not set out as a general rule that any discovery of data exempt from seizure, or any claim that such data existed among those collected, would always automatically (*uten videre*) lead to the prosecuting authority having to discontinue its perusal of the collected data.

33. Reference was made to the fact that the primary competence to decide on seizures lay with the prosecuting authority. It was, accordingly, the prosecuting authority which had the primary responsibility for ensuring that no seizure was ordered beyond what was authorised in the Code of Criminal Procedure. From this it was inferred that the prosecuting authority also had first of all to have powers to examine any data collected; it was an evident precondition, however, that in so doing the prosecuting authority would filter out and return or delete whatever data it could not lawfully keep.

34. The preparatory works to the Code of Criminal Procedure had stated that when carrying out a search the police had to look through documents in order to be able to take a decision on whether they should be seized, and that it was unavoidable that the police in that context might happen to look through documents that would be exempt from seizure.

35. The Supreme Court reiterated that in its decision of 27 March 2013 (Rt-2013-968) it had found that the aforementioned statements in the preparatory works could not apply to a situation where a lawyer's office was being searched and where the lawyer had maintained that documents in the office were subject to legal professional privilege. In such circumstances there would be a presumption that documents and other data were subject to confidentiality and should therefore be submitted to the City Court without any prior perusal or filtering.

36. In the Supreme Court's view, however, the procedure established in respect of searches and seizures of data in lawyer's offices was not to be transposed to any situation where lawyer's correspondence was discovered as part of a larger collection of data or where someone alleged that the data that had been collected comprised such correspondence. In such situations,

it was, according to the Supreme Court, more natural to apply procedures based on the guidelines which it had drawn up with regard to conversations recorded during surveillance.

37. Specifically, in its decision of 27 January 2015 (Rt-2015-81), the Supreme Court had indicated that in situations where the prosecuting authority, when reviewing surveillance data, became aware that a conversation involved or might involve a lawyer and his or her client, it could not itself listen through the conversation or read through transcripts of it in order to assess whether the conversation was subject to LPP. The Supreme Court found in that case that a system which entailed that the data at issue in such circumstances had to be sent to the regional court for examination would be compatible with Article 8 of the Convention. It did not pronounce on whether other types of filtering arrangements could be put in place meeting the requirements of that provision.

38. Returning to the case before it concerning e-mails, the Supreme Court assumed that an arrangement for filtering out data covered by LPP based on the guidelines drawn up on surveillance data in the above-mentioned decision would meet the requirements deriving from this Court's case-law under Article 8 of the Convention. If one accepted that the police were the first to peruse the data in question, the domestic courts' task would be limited to examining the data submitted to them by the police.

39. The Supreme Court refrained from commenting on how the police could sort the data, either in the case before it or in general, beyond pointing out that criteria for searching the data should be chosen in cooperation with counsel for the defence or counsel appointed to safeguard the interests of persons unaware that a search was being carried out, when a procedure to the latter effect was carried out.

40. Lastly, the Supreme Court stated that the existing legal regulation was not suited to technological developments which facilitated the seizure of large batches of data saved, for example, on computers, mobile phones and memory sticks. The Supreme Court noted that some of the difficulties had been commented on in the preparatory works relating to a proposal of a new Criminal Code, and in its view a more detailed regulation appeared pertinent (*synes nærliggende*).

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

41. The applicant complained that allowing the police to carry out an introductory examination of his smart phone in order to filter out data which might be exempt from seizure due to LPP, entailed a breach of Article 8 of the Convention, which reads:

"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. The parties' submissions

42. The Government accepted that search and seizure of the applicant's smart phone had amounted to an interference with his right to respect for his correspondence under Article 8 of the Convention.

43. As to whether the interference had been in accordance with the law, the Government maintained that the search and seizure had had a formal basis in the Code of Criminal Procedure and that the law had been accessible and foreseeable to the applicant. The relevant provisions of the Code of Criminal Procedure had been formulated with sufficient precision. Although the relevant legislation had not been applied as it was in the instant case until the Supreme Court's decision of 16 January 2017, the procedures described in that decision had not contradicted any earlier Supreme Court rulings. Legal interpretation developed through case-law, and it was essential for national courts to be able to facilitate such development in order to ensure that the law was applied correctly to cases not specifically dealt with in the relevant legislation. This held especially true in a case such as the present one, where the legislation did not deal with the issue at hand owing to technological developments unforeseen by the lawmakers.

44. Furthermore, the Government argued that the search and seizure of the applicant's smart phone had pursued the legitimate aim of preventing disorder and crime and had been necessary in order to obtain evidence in the criminal investigation in which the applicant was the aggrieved party. They also submitted that the Code of Criminal Procedure contained adequate and effective safeguards against abuse in respect of decisions to search as well as to seize objects. The preliminary filtering and deletion of LPP data had been carried out by a police officer who had not been involved in investigating the instant case.

45. The applicant submitted that the Supreme Court's decision in the present case represented a departure from well-established practice in terms of filtering out data subject to LPP, such that he could not to a reasonable degree foresee the consequences; nor had the law been accessible to him.

46. Furthermore, the applicant argued that the impugned measure was not necessary in a democratic society because the relevant legislation and practice had not afforded the applicant adequate and effective safeguards against abuse. The applicant maintained that the case concerned not judicial

authorisation before a seizure but the procedure regarding the seizure of a batch of data partly made up of information exempt from seizure, and how to filter that information out.

B. Admissibility

47. The Court notes that this 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.

C. Merits

48. The Court observes at the outset that it is undisputed between the parties that the search of the applicant's smart phone and/or the mirror image copy of it, entailed an interference with his right to respect for his correspondence under the first paragraph of Article 8 of the Convention, and considers that this cannot be called into question (see for example, *mutatis mutandis*, *Laurent v. France*, no. 28798/13, § 36, 24 May 2018). Moreover, the Court notes that the search was carried out towards the applicant in his capacity of being the aggrieved party in the pertinent investigation (see paragraph 5 above).

49. As to the question of whether the interference was in accordance with the law under the second paragraph of that provision, the Court observes that the decisions relating to the search as such, and ultimately any seizure of data from the applicant's smart phone, had a formal basis in law, namely in the provisions on searches in Chapter 15 and those on seizures in Chapter 16 of the Code of Criminal Procedure (see paragraph 29 above). In so far as it had been established that access to correspondence between the applicant and his lawyers could be obtained via the mirror image copy of his smart phone, the crux of the case is, however, whether the law in question had sufficient quality and offered sufficient safeguards to ensure that LPP was not compromised during the search and seizure procedure.

50. In that context, the Court reiterates that Article 8 § 2 of the Convention requires the law in question to be "compatible with the rule of law". In the context of searches and seizures, the domestic law must provide some protection to the individual against arbitrary interference with Article 8 rights. Thus, the domestic law must 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. Moreover, search and seizure represent a serious interference with private life, home and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject (see *Sallinen and Others v. Finland*, no. 50882/99, §§ 82 and 90, 27 September 2005).

51. 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 and of LPP (see, *inter alia*, *Sommer v. Germany*, no. 73607/13, § 56, 27 April 2017, and *Michaud v. France*, no. 12323/11, § 130, ECHR 2012). It has emphasised that professional secrecy is the basis of the relationship of trust existing between a lawyer and his client and that the safeguarding of professional secrecy is in particular the corollary of the right of a lawyer's client not to incriminate himself, which presupposes that the authorities seek to prove their case without resorting to evidence obtained through methods of coercion or oppression in defiance of the will of the "person charged" (see, for example, *André and Another v. France*, no. 18603/03, § 41, 24 July 2008). However, in its case-law, the Court has distinguished between the question of whether Article 8 has been violated in respect of investigative measures and the question of possible ramifications of a finding to that effect on rights guaranteed under Article 6 (see, for example, among many other authorities, *Dragoş Ioan Rusu v. Romania*, no. 22767/08, § 52, 31 October 2017; and *Dumitru Popescu v. Romania* (no. 2), no. 71525/01, § 106, 26 April 2007, with further references). Moreover, the Court has stressed that it is clearly in the general interest that any person who wishes to consult a lawyer should be free to do so under conditions which favour full and uninhibited discussion and that it is for that reason that the lawyer-client relationship is, in principle, privileged. It has not limited that consideration to matters relating to pending litigation only and has emphasised that, whether in the context of assistance for civil or criminal litigation or in the context of seeking general legal advice, individuals who consult a lawyer can reasonably expect that their communication is private and confidential (see, for example, *Altay v. Turkey (no. 2)*, no. 11236/06, §§ 49-51, 9 April 2019, and the references therein).

52. Proceeding to the circumstances of the instant case, the Court first of all observes that there was agreement that the mirror image copy of the applicant's smart phone contained correspondence between him and his lawyers (see paragraph 6 above). It also observes that the Code of Criminal Procedure did not include any express provisions originally designed to prescribe the procedure for such situations in which LPP could be at stake. There was however initial common ground between the police and the applicant that in order to ensure that LPP was not compromised, the data on the mirror image copy had to be sifted out by the City Court and any LPP data removed before the police could search the remainder. The legal basis for that procedure would be an application by analogy of Article 205 § 3 of the Code of Criminal Procedure (see paragraphs 6 and 29 above). The City Court appears to have shared this understanding and proceeded accordingly in order to have the filtering carried out (see paragraphs 6-7 above). Nonetheless, there was, in the absence of any express and specific rules on

the matter, subsequent disagreement as to how the City Court could go about it in practical terms, including whether it could seek assistance from the police (see paragraphs 8-11 above).

53. Thereupon, while the City Court was proceeding to sift out the LPP data in the applicant's case, the Supreme Court gave a decision in an entirely unrelated case in which the applicant had played no part, which indicated that it was – contrary to the assumptions of the applicant, the police and the City Court – in fact the police itself that should filter the data, seemingly because the Supreme Court had found that another analogy than that until then assumed correct in the instant case was more pertinent, namely application by analogy of the procedures relating to surveillance data (see paragraphs 37-38 above). After obtaining the views of the persons involved in the applicant's case concerning that new decision, the City Court concluded that owing to the Supreme Court's fresh directions it should abandon its filtering procedure and send the mirror image copy back to the police. Thereafter the police itself examined it as described in its report of 9 November 2017 (see paragraph 27 above).

54. Having regard to the foregoing observations, the Court does not find it necessary in the instant case to consider whether or under what circumstances credible claims for LPP in respect of specific data carriers entail that they must be sent to a court or another third-party independent of the police and prosecution in order to have any data covered by LPP deleted before the latter may proceed to search the data carriers. In the instant case it suffices for the Court to make the following observations.

55. Firstly, the Court takes note of the circumstance that the proceedings relating to the filtering of LPP in cases such as the present one lacked a clear basis in the Code of Criminal Procedure right from the outset, which rendered them liable to disputes such as that which followed the Supreme Court's decision of 16 January 2017. Secondly, the actual form of the proceedings could hardly be foreseeable to the applicant – notwithstanding that he was allowed to object (see paragraph 12 above) – given that they were effectively reorganised following that decision. Thirdly, and most importantly, the Court finds that the Government have not rebutted the applicant's contention that subsequently to the Supreme Court's finding in its decision of 16 January 2017 that the police should themselves examine the data carriers in cases such as the present one, the decision to apply that instruction to the applicant's ongoing case, which became final with the Supreme Court's decision of 30 June 2017 (see paragraph 26 above), meant that no clear and specific procedural guarantees were in place to prevent LPP from being compromised by the search of the mirror image copy of his phone. The Supreme Court had not given any instructions as to how the police were to carry out the task of filtering LPP, apart from indicating that search words should be decided upon in consultation with counsel; even though the claim lodged for LPP in the instant case was as such

undisputedly valid, the mirror image copy was effectively just returned to the police for examination without any practical procedural scheme in place for that purpose. As to the report of 9 November 2017 (see paragraph 27 above), it described the deletion of data in the applicant's case, but did not describe any clear basis or form for the procedure either.

56. In this context the Court emphasises that it has noted that the Government did indeed point to the procedural safeguards in place relating to searches and seizures in general; the Court's concern is, however, the lack of an established framework for the protection of LPP in cases such as the present one. On that point, the Court observes in passing that the Supreme Court, in its decision of 16 January 2017 *in fine*, also pointed to the lack of provisions suited to situations where LPP data form part of batches of digitally stored data, and indicated that it would be natural to regulate the exact issue that arose in the instant case by way of formal provisions of law (see paragraph 40 above). The Court thus notes that the issue that arose in the instant case was not as such owing to the Supreme Court's findings in that case, rather it originated in the lack of appropriate regulation as pointed out by that court.

57. Although no such regulation was in place in the applicant's case, the Court has no basis to decide whether or not LPP was actually compromised in his case, nor has the applicant submitted that it was. In the Court's view, however, the lack of foreseeability in the instant case, due to the lack of clarity in the legal framework and the lack of procedural guarantees relating concretely to the protection of LPP, 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. Having drawn that conclusion, it is not necessary for the Court to review compliance with the other requirements under that provision.

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

II. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION

59. In his application to the Court the applicant complained that the proceedings relating to the search of his smart phone amounted to a violation of the rights secured to him under Article 6 § 3 of the Convention. In his subsequent observations the applicant informed the Court that he had meanwhile been acquitted of the criminal charges against him (see paragraph 28 above), and admitted that he could therefore no longer claim to be a victim of a violation of Article 6. The Court does not find grounds for calling this into question and accordingly finds that the complaint under Article 6 must be declared inadmissible in accordance with Article 35 §§ 3 (a) and 4 of the Convention

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

60. 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

61. The applicant claimed non-pecuniary damages to an amount assessed at the Court's discretion. He did not claim pecuniary damages.

62. The Government did not contest that, should the Court find a violation of Article 8 of the Convention, there might be grounds for awarding just satisfaction in respect of non-pecuniary damage.

63. The Court, in view of the relatively technical nature of the violation found and the circumstances of the case, considers that the finding of a violation constitutes in itself sufficient just satisfaction for any non-pecuniary damage which the applicant may have suffered.

B. Costs and expenses

64. The applicant also claimed 101,937.50 Norwegian kroner – approximately EUR 9,500 for costs incurred before the Court.

65. The Government accepted that the applicant should be entitled to recover his costs in the event that the Court found a violation of Article 8 of the Convention, but maintained that the amount should be reduced since the applicant had accepted that he had no valid claim under Article 6.

66. The Court notes that the applicant requested legal aid, but did not upon its request submit the requisite information. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these were actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession, the parties' submissions and the above criteria, the Court considers it reasonable to award the sum of EUR 7,000 for the proceedings before the Court, plus any tax that may be chargeable to the applicant.

C. Default interest

67. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT

1. *Declares*, by a majority, the complaint concerning Article 8 of the Convention admissible and the remainder of the application inadmissible;

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

3. *Holds*, by six votes to one,
   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amount, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
   EUR 7,000 (seven-thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

4. *Dismisses* unanimously, the remainder of the applicant's claim for just satisfaction.

Done in English, and notified in writing on 17 December 2020, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Victor Soloveytchik	Síofra O'Leary
Registrar	President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judge Yudkivska is annexed to this judgment.

S.O.L.
V.S.

DISSENTING OPINION OF JUDGE YUDKIVSKA

I did not vote together with my learned colleagues for a violation of Article 8 of the Convention, not because I found that the legal framework at stake in the present case satisfied the requirements of Article 8 or that the appropriate procedural guarantees existed. In fact, I could have easily subscribed to their reasoning on the merits of the case.

However, I believe that the present application is inadmissible because the applicant was acquitted in the proceedings in which he claimed that his LPP had been violated. Having been acquitted, he can no longer complain of any violation of his fair trial rights – including defence rights that comprised LPP – he has lost victim status. The Court came to this conclusion in paragraph 59 of the judgment.

Having accepted that the applicant might still be a victim of a violation of his LPP, the majority, in my view, ignored the very nature of this privilege.

A lawyer-client privilege cannot be regarded as an autonomous right. That privilege, which is recognised in many international instruments and national legislations, originates from the rights of the defence and is explained – both in the doctrine and in jurisprudence – by the privilege against self-incrimination.

This Court has held many times that confidential communication with one's lawyer is protected by the Convention as an important safeguard of the right to defend oneself[1]. The lawyer-client privilege protects the integrity of legal representation itself[2]. As noted in the doctrine, this privilege has a "rule of law rationale"[3] and the right to lawyer-client confidentiality is implied by the rights to a fair trial and to legal representation[4]. It is also claimed that "the European Court of Human Rights has made clear its view that confidentiality of communications between the lawyer and client is necessary to guarantee the effectiveness of the right to legal representation"[5].

The Court has always taken the lawyer-client privilege seriously and scrutinised it meticulously. In § 38 of the *Kopp v. Switzerland* judgment[6] the Court quoted the opinion of academic writers to the effect that information not specifically connected with a lawyer's work on instructions from a party to proceedings is not covered by professional privilege[7]. It then concluded

---

[1] See *Apostu v. Romania*, no. 22765/12, § 96, 3 February 2015.

[2] H.L Ho, "Legal Professional Privilege and the Integrity of Legal Representation" (2006), 9(2) Legal Ethics, 174.

[3] Zuckerman, Civil Procedure (2003) at [15.8]-[15.10].

[4] Ho, op. cit., 163.

[5] Ibid., with a reference to Dennis, The Law of Evidence, 5th edn, Sweet & Maxwell, 2013, at p. 397.

[6] *Kopp v. Switzerland,* 25 March 1998, *Reports of Judgments and Decisions* 1998-II.

[7] With reference to G. Piquerez, *Précis de procédure pénale suisse*, Lausanne, 1994, p. 251,

that the "sensitive area of the confidential relations between a lawyer and his clients ... directly concern(s) the rights of the defence".

In *Versini-Campinchi and Crasnianski v. France*[8], the transcript of a telephone conversation which the applicant (a lawyer) had had with her client had been used in evidence in disciplinary proceedings against her. The Court found no violation of Article 8 because the domestic courts had satisfied themselves that the transcription ***had not infringed her client's defence rights***, and the fact that the former was the latter's lawyer was insufficient to constitute a violation of Article 8 of the Convention. Additionally, in *Michaud v. France*[9], the Court concludes that "the lawyer's defence role ... forms the very basis of legal professional privilege", which entails that where there has been no violation of the lawyer's defence role (which can be translated as the applicant's defence rights), one cannot claim an infringement of LLP. It is thus clear that the lawyer-client privilege is not considered separately from the rights of the defence.

Indeed, the Court has examined many complaints of violations of this privilege. Whenever a complaint concerning such an alleged violation has been submitted by a lawyer, the Court has clearly approached it from the standpoint of Article 8 (see, among many other authorities, *Petri Sallinen and others v. Finland (*no. 50882/99, 27 September 2005); *Kruglov and others v. Russia (*nos. 11264/04 and 15 others, 4 February 2020); and *Golovan v. Ukraine* (no. 41716/06, 5 July 2012)). Similar complaints submitted by suspects were mostly examined under Article 6 § 3 (c) of the Convention (see, among other authorities, *Khodorkovskiy v. Russia,* no. 5829/04, 31 May 2011; *Khodorkovskiy and Lebedev v. Russia,* nos. 11082/06 and 13772/05, 25 July 2013; and *M. v the Netherlands,* no. 2156/10, 25 July 2017), sometimes under Article 5 § 4 (see *Castravet v. Moldova,* no. 23393/05, 13 March 2007), and sometimes under Article 8 (see, among other authorities, *Piechowicz v. Poland,* no. 20071/07, 17 April 2012*,* and *Sorvisto v. Finland,* no. 19348/04, 13 January 2009) – depending on the circumstances and the applicant's initial classification.

Clearly, the nature of the interference in the lawyer-client privilege is different in cases concerning lawyers and their clients.

Explaining the scope of a lawyer's professional privilege when his/her premises are being searched and documents seized, the Court stated: "The measures complained of interfered with the first applicant's professional life: they had repercussions for his reputation as a lawyer and must have affected (his/her) wide range of personal connections..."[10]. It also "attached

---

no. 1264, and B. Corboz, "*Le secret professionnel de l'avocat selon l'article 321 CP*", *Semaine judiciaire*, Geneva, 1993, pp. 85–87.

[8] *Versini-Campinchi and Crasnianski v. France*, no. 49176/11, 16 June 2016.

[9] *Michaud v. France,* no. 12323/11, 06 December 2012.

[10] *Golovan v. Ukraine,* no. 41716/06, § 53, 5 July 2012.

particular weight to that risk since it may have repercussions on the *proper administration of justice*"[11].

As regards suspects, the Court explained the underlying rationale of the lawyer-client privilege – regardless of whether a relevant complaint was submitted under Article 8 or Article 6 § 3 (c) - by reference to ***fair trial rights***: "One of the key elements in a lawyer's effective representation of a client's interests is the principle that the confidentiality of information exchanged between them must be protected. This privilege encourages open and honest communication between clients and lawyers. The Court has previously held, in the context of Articles 8 and 6, that confidential communication with one's lawyer is protected by the Convention as an important safeguard of the right to defence"[12].

Examining such a complaint under Article 8, the Court recalled that "any person who wishes to consult a lawyer should be free to do so under conditions which favour full and uninhibited discussion. For that reason, the lawyer-client relationship is, in principle, privileged. ... Indeed, if a lawyer were unable to confer with his client without such surveillance and receive confidential instructions from him, his *assistance* would lose much of its usefulness..."[13].

It also summarised its approach in *M. v. the Netherlands* as follows:

> "85. The Court has held that an accused's right to communicate with his legal representative out of the hearing of a third person is part of the basic requirements of a fair trial in a democratic society and follows from Article 6 § 3 (c) of the Convention. If a lawyer were unable to confer with his client and receive confidential instructions from him without such surveillance, his assistance would lose much of its usefulness ...
>
> 86. The Court has also held, in the context of Article 5 § 4, that *an interference with the lawyer-client privilege and, thus, with a detainee's right to defence*, does not necessarily require actual interception or eavesdropping to have taken place...
>
> 87. The Court has further held, in the context of Article 8 of the Convention, that it is clearly in the general interest that any person who wishes to consult a lawyer should be free to do so under conditions which favour full and uninhibited discussion. It is for this reason that the lawyer-client relationship is, in principle, privileged."

The original logic of the lawyer-client privilege requires that in the course of proceedings against them suspects are able to communicate freely with their lawyers, without fear of disclosing everything relevant to the advice they are seeking. This privilege is **rooted** in the privilege against self-incrimination.

The Court underlined this interconnection in § 86, cited above, of *M. v. the Netherlands* - "an interference with the lawyer-client privilege and, ***thus***, with a detainee's ***right to defence***".

---

[11] *Wieser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, ECHR 2007-IV, § 65.

[12] See footnote 1.

[13] *Piechowicz v. Poland,* no. 20071/07, § 239, 17 April 2012.

In *Mirmotahari v. Norway* (dec.)[14], in which the domestic courts applied the same analogy of Article 205(3) as is at stake in the present case, having the City Court sift out the material before the Prosecution could search it, the Court rejected the applicant's relevant complaint under Article 8 emphasising, *inter alia*, that "the applicant has made no allegations to the effect that the adversarial procedure that had initially been practised had to be continued *for reasons relating to his own defence*".

In my view, the same applies to the present applicant's very specific Article 8 complaint, since the lawyer-client privilege is ***part and parcel of the rights of the defence***.

This would prevent any risk that the filtering of the information – albeit, as found by the majority, in the absence of procedural guarantees - might be effected with the intention of enabling the police to find evidence to be used in the trial against him.

In paragraph 51 of the judgment the majority appears to frame the LPP as an autonomous right, quoting *Altay v. Turkey (no. 2)* and suggesting that the privilege is not limited to matters relating to pending litigation only, and that individuals who consult a lawyer can reasonably expect their communication to be private and confidential whether in the context of assistance for civil or criminal litigation or in seeking general legal advice. However, this quote from *Altay v. Turkey (no. 2)* should be seen within the context of that case, which concerned a judicial decision to the effect that an official was to supervise all meetings of a detainee with his lawyer, and the full quote reads: "...not only matters relating to pending litigation but also in reporting abuses they may be suffering through fear of retaliation" (§ 50 of that judgment). Obviously, this is a logical and vitally important position in the circumstances which reflects a role to be played by the lawyer in the initial stages of proceedings when a suspect is detained (see *A.T. v Luxemburg,* § 64).

These considerations are not applicable to the present case. Mr Saber was an accused person, and he complains of an alleged violation of Article 8 rights in respect of his exchange with his lawyer in the course of criminal proceedings against him. Potentially, this could of course breach his defence rights. But it is the long-standing position of the Court that "an acquitted defendant cannot claim to be a victim of violations of the Convention which, according to him, took place in the course of the proceedings against him (see, among many others, Eur. Comm. HR, No. 13156/87, Dec. 1.07.1992, D.R. 73, p. 5).

An acquittal renders obsolete any violation of defence rights, including a violation of the lawyer-client privilege.

[14] *Mirmotahari v. Norway*, no. 30149/19, 8 October 2019.