SEARCH AND SEIZURE OF LAWYER'S COMPUTER

Milana Pisarić, PhD[1]
Faculty of Law, University of Novi Sad, Serbia

Abstract: A lawyer's duty of professional secrecy is the cornerstone of confidence relationship. The search and seizure at a lawyer's office for the purpose of criminal procedure may have repercussions not only on the interest of clients, but on the proper administration of justice. For this reason, law should protect the lawyer's duty of professional secrecy by preventing abuse or arbitrariness. The risk of impinging on this duty is particularly present when lawyer's computer, containing massive volume of electronic data, is being searched, because some of the stored files may be in connection with criminal procedure, while others may be genuinely irrelevant or contain information subject to professional secrecy. Also, some additional procedural safeguards must be taken into consideration when ordering and executing this investigative measure. The failure to comply with those safeguards would render the search of computer and seizure of the electronic data illegal or disproportionate. The author considers these legally controversial questions.

Keywords: criminal procedure, search and seizure, computer, lawyer.

INTRODUCTION

Lawyers play a significant role in democratic society based on the rule of law, which is to protect the interests of the parties, and they may not perform this task if they cannot guarantee to those, whose interests they protect, their correspondence will remain confidential. However, based on these presumptions, the search and seizure at a lawyer's office for the purpose of criminal procedure should not be prohibited, because, when a lawyer is a suspect of criminal offence or even a third party, relevant items or data of evidential importance may be found in his office. As being needed in both of these scenarios, this measure should be legally allowed and regulated by strict and considerate norms, in order to take into account the aforementioned interests.

The guaranty of secrecy of correspondence between individuals provides even stronger protection of communication between lawyers and parties. The risk of impinging on lawyer's duty of professional secrecy is particularly present when lawyer's computer, containing massive volume of electronic data is being

1 mpisaric@pf.uns.ac.rs.

searched, because some of the stored files may be in connection with criminal procedure, while others may be genuinely irrelevant or contain information subject to professional secrecy. As the search and seizure of lawyers' computer and the data stored within bear a great potential risk for lawyer's duty on professional secrecy and at the same time may result in information valuable for the criminal procedure, the question whether these investigative measures are allowed and to what extent cannot be answered without in-depth analysis of wording of law on criminal procedure in combination with the statutes regulating the position of lawyers, while differentiating the situation when the lawyer is a suspect of criminal offence and when he is only a third party.

When accessing electronic data carriers, a search can in fact come close to a targeted search for findings by chance. In case of a computer, it can be assumed that the stored data, in addition to the potentially evidence-relevant information, include considerable amounts of evidence irrelevant to the proceedings. In case of search of lawyer's computer, this may lead to a situation in which not only the data of the non-accused professionals may be affected, but also the data of clients who are in no connection to the procedural charge. Thus, it should be born in mind that some techniques and methods of digital forensics allow a differentiated search, which can often be matched with the person concerned, for example, to avoid that, when searching a law firm's computer, client files that have nothing to do with the allegation are seized only because they are on the same hard drive as for the procedure relevant data (Pisarić, 2019: 199). For that reason, relevant provisions in German law and several cases before the European Court of Human Rights are analysed.

SEARCH AND SEIZURE OF LAWYER'S COMPUTER IN GERMANY

In Germany the search serves to find and capture the perpetrator, or to find traces and objects that are temporarily confiscated because they may have the significance of evidence in criminal proceedings. German Code of Criminal Procedure (StPO) distinguishes two types of search: 1) the search of the defendant based on §102, and 2) the search of another person based on §103. The search of the law office for the purposes of criminal proceedings can be determined on both basis. However, it is to be carried out with certain legal restrictions provided by the StPO that serve to protect the trust relationship between the lawyer and the party. Some additional criteria have been created in case-law in order to justify entering this protected sphere, within the principle of proportionality. Special protection requires the most careful examination of the conditions of intervention and the principle of proportionality when ordering and executing the search of a law firm and seizure of objects found on that occasion, meaning that the aim of the search must be in a reasonable proportion to the (concrete) seriousness of the criminal offense and to the degree of suspicion that the offense is com-

mitted (Meyer-Goßner&Schmitt, 2018:491). This is also related to the potential evidential significance of the objects which are presumed to be found, as well as the degree of probability of their disclosure (Meyer-Goßner&Schmitt, 2018:494).

The seizure and confiscation of data carriers and data stored thereon is allowed, although not expressly regulated by law: data are not physical objects *per se*, nevertheless, they can be seized and confiscated according to §94, which regulates the seizure of objects of evidential significance. Investigation in cyber space is governed by the same principles: both the seizure and confiscation of e-mails at the sender or recipient computer as well as the seizure and seizure of e-mails temporarily or permanently stored on the mail server of a provider can be based on § 94 (Pisarić, 2015: 222). However, when seizing data carriers and data stored thereon, these measures must be viewed as successful for the purpose of criminal procedure, necessary (which is not the case when other less restrictive means are available) and proportional with the seriousness of the offense and the strength of the suspicion (BverfG, Beschluss von 31.8.2010 – 2 BvR 223/10).

The exclusion of some categories of persons from the duty to testify on the basis of §53 (professional secrecy holders) results in prohibition of the seizure of: 1) communication between the defendant and the defence attorney, or the lawyer; 2) the documents drawn up by the defence attorney, or the lawyer, on other circumstances to which the right relates not to testify relates; 3) other objects to which the lawyer's right not to testify refers (§97).

The German Constitutional Court dealt on several occasions with the question of how these investigative interventions directly affect the trust relationship between the professionals and their clients and what the conditions are for the admissibility of comprehensive data access for the purpose of criminal proceedings (BVerfG, Beschluss von 12. 4. 2005 - 2 BvR 1027/02).

When searching a computer, especially the lawyer's one, there is always a question of so-called findings by chance. The StPO in §108 contains the provision on *Zufallsfunde,* which ensures the usability of any evidence found at the place of search for offenses other than those which gave rise to the search itself. Although the data carrier is treated as the object of search and seizure, it is questionable if the procedural intervention regime is tailored to them, because of the considerable information content on data carrier and the fact that, as a rule, only certain data stored thereon are of evidential importance for the criminal procedure. That is why the view that the database as a whole is evidence, regardless of whether there are also other data in addition to the ultimately evidence-relevant, goes too far, because only potentially relevant evidence may be confiscated or otherwise ensured (LG Köln (12. Große Strafkammer), Beschluss von 11.08.1994 - 112 Qs 2/94). From the point of potential evidential significance, the scope of seizable evidence must not be drawn too narrowly, but on the other hand, unrestricted seizure even of data that is obviously without evidential significance would be disproportionate (BVerfG (1. Kammer des Zweiten Senats), Beschluss von 18. 3. 2009 - 2 BvR 1036/08). That is why the access to the entire database is not re-

quired and cannot be viewed as proportional, if securing the evidence-rich data can be achieved in a way that is less burdensome to those affected (Löwe-Rosenberg StPO, 2018: 27).

In one case, for example,[2] the first-instance court ordered the search and seizure of computers and electronic database of a law firm and a tax consultancy in the context of a preliminary investigation against one of its professionals. It was expected that the search would lead to the discovery of evidence, in particular the documents concerning the business relations of the accused persons with each other and the companies they operate with. The search order extended the authorities' right to access to various data stored on media, i.e. to make on-site copies of all data on the hard disks of the law firm's and tax consulting firm's computers. The police confiscated computers and seized data from the entire database of the firm. The lawyers objected that this access to the computer data had severely disturbed the trust relationship with their clients.

Constitutional complaint challenged the fact that the entire data of the law firm was copied and retained by the prosecution during the search and seizure, and was aimed to prevent law enforcement authorities from gaining the full access to them. The Constitutional Court found that, although the criminal procedural intervention regime basically allows the seizure and confiscation of data carriers and data stored thereon, the first-instance courts failed to recognize that the principle of proportionality is of particular importance in securing the data medium and all the data on it.

The principle of proportionality can be taken into account in the search, seizure and confiscation of data media and the data on them in a variety of ways. If potential information is contained on the data carriers affected by the measure, it must be checked whether it is necessary to secure the data medium and all data on it. Permanent access to the entire database is not required if the assurance of only the evidence-relevant data can be achieved in a different way. The extraction of over-the-top and confidential information that is meaningless for the process must be avoided within the limits of what is justifiable. Insofar as it is possible to differentiate the data according to their potential procedural relevance, the possibility should be examined of a separation of the potentially significant from the rest of the data. In addition to the creation of a (partial) copy with regard to the process-relevant data, consideration is given to the deletion of the data irrelevant. Also, the seizure of the entire database violated the right to informational self-determination of clients, because there are technical possibilities for an automatic processing of the collected data, and the possibility of unrestricted access to the database by law enforcement authorities could jeopardize the clients' right to confidential communication, especially when no connection between the mandate and the accused under any circumstances can be determined (BVerfG, Beschluß von 17. 7. 2002 - 2 BvR 1027/02).

2 BVerfG, Beschluß von 17. 7. 2002 - 2 BvR 1027/02.

SEARCH AND SEIZURE OF LAWYER'S COMPUTER IN CASE-LAW OF THE EUROPEAN COURT OF HUMAN RIGHTS

In several cases before the Court applicants complained in respect of the search of lawyer's computer and seizure of stored data, which represent a serious interference with the right guaranteed by Article 8 of the European Convention on Human Rights.

In the case of *Petri Sallinen and others v. Finland*[3] two searches of the law office were ordered: the first during police investigation against the lawyer's clients X and Y, in which he was considered as a witness, and the second during investigation against him, as a co-suspect of crime of X and Y. Upon the searches, X and Y were charged, but no charges were pressed against the lawyer.

In the course of search, the police perused all of the lawyer's client files, examined all floppy disks and searched, copied and seized hard disks from one of lawyer's computers - two were copied on-site and two computers were seized for later disk-copying on police premises. Three of four hard disks were returned to the lawyer and their copies were destroyed, while a copy of one hard disk remained with the police until a final court decision on lawfulness of the seizure. Lawyer's clients requested the court to revoke the seizure of the copy of the fourth hard disk arguing that the copy was of no relevance to the pre-trial investigation concerning X and Y, since it contained material relating to their instructions to the lawyer.

The lawyer and his clients complained to the Court that the search and seizure of privileged material and retention by the police of a copy of the fourth hard disk had breached Article 8 of the Convention. The Court examined whether this interference was in accordance with the law: it found that the interference had a legal basis in the Finnish law, and that the accessibility of the law was not problematic. However, even there is a general legal basis for the measures in the Finnish law,[4] the absence of applicable regulations specifying with an appropriate degree of precision the circumstances in which privileged material could be subject to search and seizure deprived the applicants of the minimum degree of protection to which they were entitled under the rule of law. The relationship between laws read together was unclear and gave rise to diverging views on the extent of the protection afforded to privileged material in searches and seizures. Therefore, the search and seizure measures were carried out without proper legal safeguards.

3 ECHR Judgment in case of Petri Sallinen and others v. Finland (Application no. 50882/99) of 27 September 2005.

4 A document shall not be seized for evidential purposes, if it may be presumed to contain information in regard to which a person is not allowed to give evidence (chapter 4, section 2, and subsection 2 of the Coercive Measures Act). A counsel may not testify in respect of what a client has told him or her for the purpose of pleading a case (chapter 15, section 23 of the Code of Judicial Procedure). The Court found these provisions unclear, while it is not clear whether pleading a case covers only the relationship between a lawyer and his/her clients in a particular case or their relationship generally, which permits various interpretations as to the extent to which privileged material could be subject to search and seizure.

In the case of *Wieser and Bicos Beteiligungen GmbH v. Austria*[5] in investigating illegal trade in medicaments against a number of persons and companies in Italy, invoices addressed to company B had been found. Company B is owned by company A whose owner and general manager was a lawyer in Salzburg. Upon the request for legal assistance from the Italian authorities, Salzburg Regional Court issued a search warrant of both companies' offices based in the law office, in order to seize all business documents which could reveal contacts with the suspected persons and companies. One group of officers searched the law office for hard-copies of files relating to company A or company B, in the presence of the lawyer and a representative of the Bar Association. All documents were shown to them before seizure and if they objected to the immediate examination of a document, it was sealed and deposited with the regional court, as required by Article 145 of the Code of Criminal Procedure.[6] All seized and sealed documents were listed in a search report signed by the lawyer and the officers and handed over to the investigating judge, who opened them in the presence of the lawyer: some were copied and added to the file, and some were returned to the lawyer on the ground that their use would impinge on his duty of professional secrecy. At the same time, another group of officers examined the lawyer's computer and copied several files to disk. The administrator of computer system was called upon to provide some technical assistance but left after about half an hour, while the representative of the Bar Association attended that search only briefly. When terminated the search of the computer, the officers left without drawing up a search report and without informing the lawyer about the results of the search. The report drawn up later that day indicated that a complete copy of the server was not made, as the search was carried out using only the names of the companies involved and the names of the suspects in the Italian proceedings. As a result, a folder named Company B containing ninety files and a file containing one of the search items were copied, as well as retrieved, previously deleted files corresponded to the search items. These disks and printouts of files were handed over to the investigating judge.

The lawyer complained to the domestic courts, as the search of his premises and the seizure of electronic data violated his right and duty of professional secrecy under section 9 of the Lawyers Act in conjunction with Article 152 of the Code of Criminal Procedure,[7] as some officers had proceeded unobserved to examine and subsequently copy electronic data. These complaints were dismissed.

5 ECHR Judgment in case of Wieser and Bicos Beteiligungen GmbH v. Austria (Application no. 74336/01) of 16 October 2007.

6 When searching through (paper) documents steps must be taken to ensure that their content does not become known to unauthorised persons: if the owner of the documents does not want to permit their being searched, they shall be sealed and deposited with the court, and the Review Chamber must determine immediately whether they are to be examined or returned. According to case-law, these provisions apply also to the search and seizure of electronic data: if the owner of disks or hard disks on which data is stored objects to their being searched, the data carriers are to be sealed and the Review Chamber must decide whether they may be examined.

7 This article exempts lawyers from the obligation to give evidence as witnesses in respect of information given to them in the exercise of their profession. Also, in the courts' case-law it

The applicants (lawyer and company A) alleged that the search and seizure of electronic data in the context of a search of their premises violated their right under Article 8 of the Convention.

The Court found that, although the Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data, it contains detailed provisions for the seizure of objects and specific rules for the seizure of documents, which apply to the search and seizure of electronic data, as established in the domestic courts' case-law. The measures were ordered in the context of criminal proceedings, and therefore served a legitimate aim (prevention of crime). The search warrant was based on reasonable suspicion, it limited the documents or data to be looked for in a reasonable manner and the search remained within these limits (the officers searched for documents or data containing either the word Company A or Company B or the names of any of the suspects). The question was whether they were proportionate to this aim and whether provided procedural safeguards designed to prevent any abuse or arbitrariness and to protect the lawyer's duty of professional secrecy were adequately complied with.

The Court found that the safeguards had been complied with in respect of the hardcopies of the documents seized, but not in respect of the electronic data, so the lawyer's rights were restricted.[8] As for violation of lawyer's right to professional secrecy, although he was not the counsel of company A or B, he was the counsel for numerous companies whose shares were held by the company A. The same reason for which some paper documents were returned to him by the investigating judge (as being subject to professional secrecy), had to be applied to electronic data as well, as they might contained some information subject to professional secrecy. The Court concluded that the failure to comply with these procedural safeguards made the search and seizure of the lawyer's electronic data disproportionate to the legitimate aim.

In the case of *Robathin v. Austria*[9] in course of criminal investigation against a lawyer in connection with a series of thefts and frauds, an investigating judge issued a search warrant of his law office. The lawyer, his defence counsel and a representative of the Bar Association were present. The relevant data covered by the search warrant were copied and saved on separate disks. Although the representative of the Bar Association insisted that it was technically possible, by using appropriate search criteria, to search for and copy only those files which corresponded to the criteria set out in the search warrant, the search of computer was extended to all stored data which were also copied. Following the search, a review chamber authorised the examination of all the materials, after noting that the

is established that documents which contain information subject to professional secrecy may not be seized and used in a criminal investigation.

8 The member of the Bar Association was only temporarily present during the search of the computer and did not properly exercise his supervisory function as regards the electronic data; the officers left without informing the lawyer or the representative of the Bar Association of the results of the search, and the report was not drawn up at the end of the search.

9 ECHR Judgement in case of Robathin v. Austria (Application no. 30457/06) of 3 July 2012.

data had been seized in the context of preliminary investigations and that a lawyer could not rely on his duty of professional secrecy and the attendant guarantees of Article 152 § 1 of the Code of Criminal Procedure[10] when he himself was the suspect. Ultimately the lawyer was acquitted of the offences.

The Court found that the search and seizure were in accordance with the law, pursued a legitimate aim and were carried out upon a warrant based on reasonable suspicion. However, the warrant was not reasonably limited, because it was written in very broad terms, authorizing, in a general and unlimited manner, the search and seizure of all documents, and hence, it did not provide protection against abuse or arbitrariness. Also, the Review Chamber gave only very brief and general reasons when authorising the search of all the electronic data - it did not address the question whether it would be sufficient to search only those files which contained relevant data, nor did it give any specific reasons for its finding that a search of all of the applicant's data was necessary for the investigation. Therefore, the search of all of the lawyer's electronic data was not proportionate and represents a violation of Article 8 of the Convention.

In the case of *Sérvulo & Associados - Sociedade de Advogados, Rl v. Portugal*[11] in course of investigation against several persons, including a lawyer who worked on behalf of the law firm (the applicant), on suspicion of corruption, acquisition of prohibited interests and money laundering, two warrants for searches of the law firm's computer system were issued. The search order allowed the authorities to seize stored data on the basis of a list of 35 keywords, including the names of companies and banks linked to the investigation and terms such as "financial contributions" and "funding". After the search is finished, the report was made, listing all the seized documents and data-carriers.

The Court of Appeal found that keywords were related to the investigation, that the information seized was relevant, and that there had been no flagrant breach of legal professional secrecy. The seized computer files and emails were sent back to the investigating judge, who, after viewing them in the presence of law firm's partners, a public prosecutor, a police officer and three IT experts, ordered the deletion of copy of 850 records on hard disks and DVDs, considered to be private, to be covered by professional secrecy or to have no direct bearing on the case. The original data-carriers were returned to the law firm, and the rest of 89.000 files and 29.000 e-mails were further analysed. Ultimately, the investigation was dropped.

The law firm and several lawyers complained to the ECHR, because keywords in the warrants would lead to finding of a disproportionate number of irrelevant and protected data on clients not related to the investigation.

10 This article exempts lawyers from the obligation to give evidence as witnesses in respect of information given to them in the exercise of their profession.
11 ECHR Judgement in case of Sérvulo & Associados - Sociedade de Advogados, Rl v. Portugal (Application no. 27013/10) of 3 September 2015.

The Court found that the scope of warrants were too broad, because some of the keywords enumerated in the warrants were either in general use or routinely used in a law firm specialised in financial law. However, the Court found that all the procedural safeguards against abuse, arbitrariness and breaches of legal professional secrecy in the course of search and seizure operations in law firms, provided by the Code of Criminal Procedure and the Bar Association statutes, were adequately and sufficiently applied, thus there was no violation of Article 8 of the Convention.

CONCLUSION

While professional secrecy serves to protect the special relationship between a lawyer and a client, it does not protect the lawyer himself against criminal prosecution or the measures in connection with such prosecution. However, in both cases, and even when search and seizure of lawyer's computer is carried out for the purpose of investigation of a serious crime of which the lawyer is a suspect, he should be treated differently, with regard to lawyer's general obligation of professional secrecy and confidentiality. As, at the same time, these measures represent a serious interference with private life, home and correspondence, they must be accordingly based on a law that is particularly precise and clearly determines the extent of the protection afforded to privileged material.

The search and seizure of lawyer's computer serve a legitimate aim when ordered in the context of criminal proceedings. However, the search warrant should be based on reasonable suspicion, should limit in a reasonable manner the documents or data looked for and the execution ought to remain within these limits. But there is also the question whether they are proportionate to this aim and whether provided procedural safeguards designed to prevent any abuse or arbitrariness and to protect the lawyer's duty of professional secrecy are adequately complied with. As for the necessity of the interference, the question whether these measures are proportionate to the legitimate aim pursued, these procedural safeguards should be provided for by the law: the search is based on a warrant issued by a judge on reasonable suspicion, the scope of the warrant is reasonably limited, and the search is carried out in the presence of an independent observer in order to ensure that materials subject to professional secrecy is removed. The search carried out in this manner minimises the risk of impinging on lawyer's right and duty of professional secrecy. The failure to comply with some of these procedural safeguards would render the search and seizure of the electronic data disproportionate to the legitimate aim pursued.

REFERENCES

1. BVerfG (1. Kammer des Zweiten Senats), Beschluss von 18. 3. 2009 - 2 BvR 1036/08.
2. BVerfG, Beschluss von 12. 4. 2005 - 2 BvR 1027/02.
3. BVerfG, Beschluß von 17. 7. 2002 - 2 BvR 1027/02.
4. BverfG, Beschluss von 31.8.2010 – 2 BvR 223/10.
5. ECHR, Judgement in case of Robathin v. Austria (Application no. 30457/06) of 3 July 2012.
6. ECHR, Judgement in case of Sérvulo & Associados - Sociedade de Advogados, Rl v. Portugal (Application no. 27013/10) of 3 September 2015.
7. ECHR, Judgment in case of Petri Sallinen and others v. Finland (Application no. 50882/99) of 27 September 2005.
8. ECHR, Judgment in case of Wieser and Bicos Beteiligungen GmbH v. Austria (Application no. 74336/01) of 16 October 2007.
9. LG Köln (12. Große Strafkammer), Beschluss von 11.08.1994 - 112 Qs 2/94.
10. *Löwe-Rosenberg StPO*, Volume 3-1, 27. Auflage 2018.
11. Pisarić, M. (2015). Pretresanje računara radi pronalaska elektronskih dokaza. *Zbornik Pravnog fakulteta u Novom Sadu*, 49(1), 2015-238.
12. Pisarić, M. (2019). *Elektronski dokazi u krivičnom postupku*. Novi Sad: Centar za izdavačku delatnost Pravnog fakulteta u Novom Sadu.
13. Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 3 des Gesetzes vom 18. April 2019 (BGBl. I S. 466) geändert worden ist.
14. Meyer-Goßner/Schmitt, *Strafprozessordnung mit GVG und Nebengesetzen*, 61. Auflage, C.H. Beck 2018.