UDK 621.396/.398:004.6]:343.1
621.396/.398:004.6]:349.2

Original Research Paper

SEARCHING THE PERSONAL COMPUTER: CRIMINAL PROCEDURE AND LABOUR LAW ASPECTS

Turanjanin Veljko
Associate professor, University of Kragujevac, Faculty of Law, Serbia
vturanjanin@jura.kg.ac.rs

Turanjanin Jovana
University of Kragujevac, Court of the Appeal in Kragujevac
jovanaturanjanin9gmail.com

Abstract

In the paper, the authors explain the search of the computer from the aspect of criminal procedure and labour law. The 21st century is marked by an increasingly frequent need to search for computers as devices for automatic data processing. The Code of Criminal Procedure of Serbia, in addition to the search of devices for automatic data processing, also recognizes the computer search of data as a special evidentiary action. Special evidentiary actions are also a permanent subject before the European Court of Human Rights. However, in addition to the criminal procedure aspect, the labour law aspect of the search of a personal computer by the employer is also important. Therefore, the authors analyse the mentioned matter both from the aspect of national laws and from the aspect of human rights protection.

Keywords: *surveillance, computer, data search, right to privacy*

1. Introduction

Modern technologies benefit both criminals and everyone who fights crime. At the same time, modern surveillance systems, although they can prevent criminal behaviour, can also have a very intrusive effect on human rights and freedoms. Video surveillance, without a doubt, represents a valuable tool to protect people and property from damage and theft. Further, prosecuting authorities around the world have increasingly come to rely on the notion of seriousness to loosen the safeguards built into the criminal justice system, most notably around the protection that is usually granted to suspects, shifting towards a risk–security–seriousness paradigm, while simultaneously increasing the use of surveillance and closed-circuit television; in turn, these are often at odds with the notion of respect for private life, as exemplified in Article 8 of the European Convention on Human Rights and Fundamental Freedoms.

If we look at the jurisprudence of the European Court of Human Rights, we can see an increasing number of judgments that deal with rights from the employment relationship and in connection with modern surveillance technologies. At the same time, in criminal proceedings, it is necessary to fulfill a slightly larger number of conditions in order for evidentiary actions related to digital technologies to be legal. In this field, the computer stands out in particular. Therefore, we have divided this paper into two parts. In the first part,

we deal with the criminal procedural aspects of computer searches, and there we discussed the temporary confiscation of items, searches, and we briefly mentioned the possibilities of computer surveillance during special evidentiary actions. In the second part of the paper, we dealt with labour law aspects of computer surveillance, analysing the well-known and new judgment of the European Court of Human Rights in the case of *Libert v. France.*

2. Automatic data processing devices and Serbian Criminal Procedure Code

2.1. Temporary seizure of objects

Devices for automatic data processing appear more and more often in criminal proceedings. Sometimes openly, sometimes through the interpretation of certain provisions of the Criminal Procedure Code, we can come across legal regulation, which in practice can cause problems. But primarily, here it is necessary to start from the legal definition of electronic data. Accordingly, electronic record is the audio, video or graphical data in electronic (digital) form; electronic address is a set of characters, letters, numbers and signals intended for determining the origin of a connection; electronic document is defined as a set of data which is defined as an electronic document under the law regulating electronic documents; and under the term of electronic signature we find the set of data which is defined as an electronic signature under the law regulating the electronic signature (Article 2 points 29-32).

The authority conducting proceedings shall temporarily seize objects which must be seized under the Criminal Code or which may serve as evidence in criminal proceedings and secure their safekeeping. The decision on the temporary seizure of funds which are the object of a suspicious transaction and their placement in a special account for safekeeping shall be issued by the court. Among the objects, automatic data processing devices and equipment on which electronic records are kept or may be kept, are also included (Article 147 of the CPC).

A person holding these objects shall be required to make possible to the authority conducting proceedings access to the objects, to provide information needed for their use and to surrender them at the request of the authority. Prior to seizing the objects, the authority conducting proceedings shall, if needed, inspect the objects, in the presence of a professional. This person refusing to make possible access to objects, to provide information needed for their use or to surrender them, may be fined by the public prosecutor or the court with up to 150,000 dinars (approximately 1.280,00 EUR), and if after being fined still refuses to fulfil his/her duty, may be punished with the same fine once again. The same shall be done in respect of a responsible person in a public authority, a military facility or an enterprise or other legal person. An appeal against the ruling pronouncing a fine shall be decided on by the judge for preliminary proceedings or the panel. An appeal shall not stay execution of the ruling (Article 148).

The following are exempted from duty to surrender objects: defendant and a person who is exempted from the duty to testify (Article 149) (it is a person who, with his statement, would violate the duty to keep secret information, until the competent authority, i.e. the person of the public authority, revokes the secrecy of the information or releases him from that duty; a person whose statement would violate the duty to keep professional secrecy (religious confessor, lawyer, doctor, midwife, etc.), unless he is released from that duty by a special regulation or statement of the person in whose favour the keeping of the secret was established and the person whom the defence counsel has entrusted to him as his defence counsel. However, the court may, at the proposal of the defendant or his defence counsel, decide to examine a person who is excluded from the duty of testifying).

A certificate shall be issued to a person from whom objects are seized, in which they shall be described, the locations where they were found indicated, data on the person from whom the objects are

being sized given, and the capacity and signature of the person conducting the action given. Documents which may serve as evidence shall be listed, and if that is not possible, the documents shall be placed under a cover and sealed. The owner of the documents may place his/her seal on the cover. The person from whom the documents were seized shall be summoned to attend the opening of the cover. If failing to respond or if absent, the authority conducting proceedings shall open the cover, inspect the documents and make a list thereof. When inspecting the documents, care must be taken for unauthorised persons not to be allowed to gain insight into the content thereof (Article 150).

Objects temporarily seized during proceedings shall be returned to their holder if the reasons for which the objects were temporarily seized cease to exist, and the reasons for their confiscation do not exist (Article 535). If the object is indispensable for the holder, it may be returned to him/her even before the cessation of the reasons for which it was seized, with an obligation of bringing it in at the request of the authority conducting proceedings. The public prosecutor and the court shall, *ex officio* look after the existence of reasons for the temporary seizure of objects (Article 151).

2.2. Search

An issue of search and seizure is deeply rooted in criminal procedure systems worldwide as well as in human rights system (Grabenwarter, 2013, 112). Nowadays, this evidentiary action faces a number of challenges. One of them is certainly digital evidence. Over the past few decades, advancements in technology have led to an unparalleled expansion of the ways in which we utilize electronic devices in our daily lives: smartphones, tablets, laptops, smartwatches, and the internet of things in our homes, cars, workplaces, and the growing number of smart cities. ICT (information and communication technology) technologies are now practically required in daily life; most people find it hard to envision living without them (Nuzzo, 2022, 151-152). Precisely because it deeply encroaches on human rights and freedoms, this evidentiary action worldwide requires deep attention and the fulfilment of appropriate conditions (Pollock, 2012, 15).

According to the Serbian Criminal Procedure Code, a search of a dwelling or other premise or a person may be performed if it is probable that the search shall result in finding the defendant, traces of the criminal offence or objects of importance for the proceedings. A search of a dwelling or other premise or a person shall be performed on the basis of a court order or exceptionally without an order, on the basis of a legal authorization (Bejatović, 2018). The search of automatic data processing devices and equipment on which electronic records are kept or may be kept, shall be undertaken under a court order and, if necessary, with the assistance of an expert (Article 152). In essence, it is clear here that searches of devices for automatic data processing can only take place on the basis of a court order and only with the help of an expert.

During a search, objects and documents connected to the purpose of the search shall be temporarily seized. If during a search object are found which are not connected to the criminal offence for which the search was undertaken, but which indicate another criminal offence prosecutable *ex officio*, they shall be described in the record and temporarily seized, and a receipt on the seizure shall be issued immediately. If the search was not undertaken or attended by the public prosecutor, the authority which performed the search shall notify the public prosecutor thereof immediately. If the public prosecutor finds that there are no grounds to initiate criminal proceedings or if the reasons for which the objects were temporarily seized cease to exist, and the reasons for their confiscation do not exist (Article 535), the objects shall immediately be returned to the person from whom they were seized (Article 153).

Devices for automatic data processing are devices that enable permanent memorization of data and programs so that they can be used later (Pavišić, 2011, 538). The devices and equipment on which electronic

records are stored or can be stored are the carriers of electronic records, i.e., sound, video and graphic data obtained in digital form (Ilić, Majić, Beljanski, & Trešnjev, 2013, 389). These devices can be the subject of both investigation and expertise.

During a search, objects and documents connected to the purpose of the search shall be temporarily seized. If during a search object are found which are not connected to the criminal offence for which the search was undertaken, but which indicate another criminal offence prosecutable *ex officio*, they shall be described in the record and temporarily seized, and a receipt on the seizure shall be issued immediately. If the search was not undertaken or attended by the public prosecutor, the authority which performed the search shall notify the public prosecutor thereof immediately. If the public prosecutor finds that there are no grounds to initiate criminal proceedings or if the reasons for which the objects were temporarily seized cease to exist, and the reasons for their confiscation do not exist (Article 535), the objects shall immediately be returned to the person from whom they were seized (Article 154).

2.3. Special investigative measures

Special investigative measures today represent one of the most important parts of the fight against serious criminal offences. However, their improper use endangers fundamental human rights, especially the right to privacy and the right to a fair trial. The European Convention on Human Rights and Fundamental Freedoms in Article 8 prescribes that everyone has the right to respect for his private and family life, his home and his correspondence; 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 (Turanjanin, 2022). There are many aspects of Article 8, so case-law regarding Article 8 is very comprehensive (de Hert, 2005, 73). This is also a spot where it is easy to find connection with labour rights under the same article. However, here the search of the computer is possible only in an indirect way, but it is certainly possible.

3. Labour context: Opening of personal files stored on a professional computer

Supervision of employees and their workplace is an increasingly common topic in the implementation of human rights protection. Surveillance can be carried out in different ways, whether it is video surveillance (Turanjanin, 2020), surveillance of the company's property or surveillance of the business computer.

The case *Libert v. France* concerned the dismissal of an SNCF (French national railway company) employee after the seizure of his work computer had revealed the storage of pornographic files and forged certificates drawn up for third persons (Libert v. France, 2018). We will explain it in detail. In the first place, hired in 1976 by the national railway company ("SNCF"), the applicant most recently held the position of deputy head of the surveillance brigade of the Amiens region. He indicates that in 2007, he had reported to management the behaviour of one of his subordinates, who, according to him, had adopted outrageous language against a colleague. The person concerned having filed a complaint against him, he was indicted for slanderous denunciation. He was then suspended from his duties by the SNCF in light of this indictment. The procedure having, after several months, resulted in a dismissal of the case, the applicant informed his management of his wish to return to his former position. In response, he was asked to consider moving to another position. However, he maintained his request.

On the day of his reinstatement, March 17, 2008, the applicant noticed that his professional computer had been seized. Summoned by his superiors, he was informed on April 5, 2008 that the hard drive of this computer had been analysed and that there had been found "certificates of change of residence written on the header of the SUGE brigade of Lille and on benefit of third parties", as well as numerous files containing pornographic images and films. It appears from the judgment of the Amiens Court of Appeal of December 15, 2010 (paragraphs 14-15 below) that the person who had replaced the applicant during his suspension from his post had found on this computer "documents which had attracted his attention", and that he had informed his superiors in March 2007 and January 2008.

A request for written explanations was sent to the applicant on 7 May 2008. He replied that in 2006, following problems affecting his personal computer, he had transferred the contents of one of his USB sticks to his computer professional. He added that the pornographic files had been sent to him by people he did not know, via the SNCF Intranet. The applicant was summoned to a disciplinary interview, which took place on May 21, 2008. On June 9, 2008, he was informed by the "resource management director" of the Amiens management that he was the subject of a proposal for dismissal from the executives and that he was going to be brought before the disciplinary council. The latter meets on July 15, 2008.

On July 17, 2008, the regional director of SNCF decided to remove the applicant from management. His decision reads as follows: "(...) the analysis of the files on the hard drive of [the applicant's] professional computer, used in the context of his duties, contained: - a certificate of change of residence, signed with his name, certifying the transfer on 01/11/2003 of Ms. Catherine [T.] to the SUGE brigade in Lille; the original of this certificate sent to ICF Nord-Est made it possible to shorten the notice period for vacating one's accommodation; - a certificate of change of residence, issued on the letterhead of the Ministry of Justice in the name of Mr. [S.-J.], director of the Fresnes remand centre, certifying the transfer of Mr. [P.] Frédéric in the Strasbourg remand centre, from November 1, 2006; - a draft of documents established under the name of Michel [V.], director of SOCRIF, attesting to his financial situation with regard to this company; - a very large number of files containing pornographic images and films (zoophilia and scatophilia). These facts are contrary to the obligation of particular exemplarity linked to the functions he held within SUGE, and to the provisions: - article 5.2 of RH 0006 relating to the principles of behaviour of SNCF agents; - the general framework RG 0029 (information systems security policy – user charter); - RA 0024 "code of ethics" – how to behave with regard to the company's information system; - article 441-1 of the penal code.

On October 28, 2008, the applicant submitted a request to the Amiens industrial tribunal for his dismissal to be declared devoid of any real and serious cause. On May 10, 2010, the industrial tribunal judged that the decision to remove the applicant from the executive ranks was justified and, consequently, rejected his requests. On December 15, 2010, the Amiens Court of Appeal essentially confirmed this judgment. It ruled in particular as follows: "(...) Whereas [the applicant] maintains that the SNCF violated his private life by opening in his absence elements identified as personal on his computer; Whereas it is the rule that the documents held by the employee in the company office are, except when he identifies them as being personal, presumed to have a professional nature, so that the employer can have access to them outside; Whereas it appears from the SEF report that the pornographic photos and videos were found in a file called "laughter" contained in a hard drive called "D:/personal data"; Whereas the SNCF explains without contradiction that the "D" disk is called by default "D:/data" and is traditionally used by agents to store their professional documents; Whereas an employee cannot use an entire hard drive, intended to record professional data, for private use; that the SNCF was therefore entitled to consider that the designation "personal data" appearing on the hard drive could not validly prohibit access to this element; that in any event, the generic term "personal data" could relate to professional files handled personally by the employee and therefore did not explicitly designate elements relating to his private life; that this was also the case, the

analysis of the hard drive having revealed numerous documents of a professional nature ("LGV photos" file, "warehouse photos" etc.).

Whereas furthermore that the term "laughter" does not clearly confer to the file thus designated a necessarily private character; that this designation may relate to exchanges between work colleagues or to professional documents, kept as "bloopers", by the employee; that the employer also pertinently recalls that the user charter provides that "private information must be clearly identified as such ("private" option in the outlook criteria)" and that the same applies to "private" information. media receiving this information ("private" directory); that the first judge therefore rightly considered that the file was not identified as personal;

The Court of Appeal further found that the removal was not disproportionate. It emphasized in this regard that both the SNCF code of ethics and the internal standards recalled that agents must use the IT resources made available to them for exclusively professional purposes, with occasional private use only being tolerated. However, applicant had "massively contravened these rules, not hesitating to use his professional equipment to create a false document". According to it, these actions were all the more serious as his status as an agent responsible for general surveillance should have led him to exhibit exemplary behavior. The applicant appealed to the Court of Cassation. He claimed in particular that Article 8 of the Convention had been violated. The social chamber of the Court of Cassation rejected the appeal by a judgment of July 4, 2012. It ruled as follows:

"(...) whereas if the files created by the employee using the computer tool made available to him by the employer for the needs of his work are presumed to be of a professional nature, so that the employer is entitled to open them outside his presence, unless they are identified as being personal, the name given to the hard drive itself cannot confer a personal character to all of the data it contains; that the court of appeal, which held that the name "D:/personal data" of the hard drive of the employee's computer could not allow him to use it for purely private purposes and thus prohibit its use access to the employer, legitimately deduced that the disputed files, which were not identified as being "private" according to the recommendations of the IT charter, could be regularly opened by the employer."

The applicant complained in particular that his employer had opened, in his absence, personal files stored on the hard drive of his work computer. The Court held that there had been no violation of Article 8 of the Convention, finding that in the present case the French authorities had not overstepped the margin of appreciation available to them. The Court noted in particular that the consultation of the files by the applicant's employer had pursed a legitimate aim of protecting the rights of employers, who might legitimately wish to ensure that their employees were using the computer facilities which they had placed at their disposal in line with their contractual obligations and the applicable regulations. The Court also observed that French law comprised a privacy protection mechanism allowing employers to open professional files, although they could not surreptitiously open files identified as being personal. They could only open the latter type of files in the employee's presence. The domestic courts had ruled that the said mechanism would not have prevented the employer from opening the files at issue since they had not been duly identified as being private. Lastly, the Court considered that the domestic courts had properly assessed the applicant's allegation of a violation of his right to respect for his private life, and that those courts' decisions had been based on relevant and sufficient grounds (Libert v. France, 2018).

Conclusion

The video surveillance system is rightfully considered a powerful tool for fighting crime and for protection of property. However, this is still a sensitive matter. From the perspective of human rights, this kind of surveillance does violate them to a certain degree. A balance must be established between the loss of privacy and the seriousness of threats that the system is installed to mitigate. We have divided this paper into two parts. In the first part, we habe explained the criminal procedural aspects of computer searches, and there we have discussed the temporary confiscation of items, searches, and we briefly mentioned the possibilities of computer surveillance during special evidentiary actions. In the second part of the paper, we dealt with labor law aspects of computer surveillance, analyzing the well-known and new judgment of the European Court of Human Rights in the case of *Libert v. France*. Through the analysis of both the legal provisions and the jurisprudence of the European Court of Human Rights, we can notice the court's effort to reconcile the right to privacy of the individual, who is often in the position of the defendant (worker), and the rights of the state, i.e., the company where the worker is employed.

BIBLIOGRAPHY

Bejatović, S. (2018). Krivično procesno pravo. Beograd: Službeni glasnik.

de Hert, P. (2005). Balancing security and liberty within the European human rights framework. A critical reading of the Court's Case law in the light of surveillance and criminal law enforcement strategies after 9/11. Utrecht Law Review 1, 68–96.

Grabenwarter, C. (2013). European Convention on Human Rights: Commentary. Basel: Verlag.

Ilić, G., Majić, M., Beljanski, S., & Trešnjev, A. (2013). Criminal Procedure Code: A Commentary. Belgrade: Official Gazette.

Libert v. France, Application no. 588/13 (ECtHR February 22, 2018).

Nuzzo, V. D. (2022). Search and Seizure of Digital Evidence: Human Rights Concerns andNewSafeguards. In L. B. Winter, & S. Ruggeri, Investigating and Preventing Crime in the Digital Era: New Safeguards, New Rights (pp. 119-150). Cham: Springer.

Pavišić, B. (2011). Komentar Zakona o kaznenom postupku. Rijeka: Dušević & Kršovnik d.o.o.

Pollock, J. (2012). Criminal Law. London and New York: Routledge

Turanjanin, V. (2020). Video Surveillance of the Employees Between the Right to Privacy and Right to Property After López Ribalda and Others v. Spain. University of Bologna Law Review, 5(2), 268–293. https://doi.org/10.6092/issn.2531-6133/10514.

Turanjanin, V. (2022). Special investigative measures: Comparison of the Serbian Criminal Procedure Code with the European Court of Human Rights Standards. The International Journal of Evidence & Proof, 26(1), 34-60. https://doi.org/10.1177/13657127211055.