## 8. Seizure and search of an electronic device

Literature

Lang, Andreja: Investigating communication and electronic privacy, Proceedings of the 2nd Conference of Criminal Law and Criminology, GV Založba, Ljubljana 2009, pp. 175–183; Selinšek, Liljana: Electronic evidence – traps and opportunities, in: Pravna praksa, 2008, vol. 27, no. 27, pp. 12–15; Selinšek, Liljana: Handling electronic devices under the ZKP-J: only the police or also other state bodies?, in: Pravna praksa, 2010, vol. 29, no. 3/4, pp. 18–19; Završnik, Aleš (ed.): Crime and technology, Institute of Criminology at the Faculty of Law in Ljubljana, 2010.

### 8.1. Definition

The seizure and search of an electronic device (Article 219a of the ZKP) are investigative actions intended to (a) provide physical control over an electronic device and (b) extract the data contained in the electronic device. An electronic device is considered to be all electronic data carriers in digital form, such as telephones, fax machines, computers, floppy disks, optical media (CD, DVD, blue-ray), memory cards and keys, etc. (first paragraph of Article 219a of the ZKP).

The regulation of the seizure and search of an electronic device is the legislator's response to the position of the Supreme Court of the Republic of Slovenia (Up-106/05) that the limitations of interference with communication privacy (second paragraph of Article 37 of the URS) must also be taken into account when obtaining data from electronic communication devices, i.e. a specific legal regulation and a prior court decision. Since in practice it is likely that an electronic device will also contain data on the communication of its owner (for example, e-mail, SMS messages, call data, etc.) and it is not possible to ensure in advance that the interference will be limited to other data only, the provisions on the search of an electronic device uniformly regulate the acquisition of all data stored in digital form on electronic devices. The special regulation of the acquisition (seizure, security and search) of digital data is dictated by the special characteristics of proving with electronic digital evidence (for more details on electronic evidence, see section 4.5 of the Special Part).

The purpose of searching an electronic device is to obtain data stored on the electronic device. Before the data is accessed as part of the search, it must be properly secured (see Section 3.3 of the Special Part).

### 8.2. Assumptions

The seizure and search of an electronic device shall be carried out if there are reasonable grounds for suspecting the commission of a criminal offence and it is likely that the electronic device contains data necessary for the discovery, identification or arrest of a suspect or the discovery of traces of a criminal offence, or it is likely that the data on the device can be used as evidence in criminal proceedings (first paragraph of Article 219a of the ZKP).

Thus, two alternative legal bases are provided for such an investigation: -

prior written consent of the owner and users of the device known and reachable to the police, i.e. those who have a reasonable expectation of privacy in relation to the data on the device (second paragraph of Article 219.a of the

ZKP), or - a court order issued by the court at the proposal of the state prosecutor.

The investigating judge cannot therefore issue such an order ex officio.

The court order must be in writing and reasoned. Both the order and the proposal must contain: –

information that allows the identification of the electronic device to be searched,

– justification of the reasons for the
investigation, – definition of the content of the data being
sought, and – other important circumstances that dictate the use of this investigative action and determine the method of its execution (for example, a professionally qualified person to execute it).

In the event of an immediate and serious danger to people or property, an investigation may also be ordered orally, upon an oral request, if a written order cannot be obtained in time (the fifth paragraph of Article 219.a of the ZKP). The investigating judge shall make an official note of the order and the request, and shall issue a written order within twelve hours. Otherwise, the police shall destroy the stored and copied data in a record and notify the investigating judge, the public prosecutor and the owner or users of the device thereof.

Even in the case of an oral motion, the investigating judge must assess whether there is indeed an immediate and serious threat to the safety of people and property. Given such diction, it is important to strictly interpret every word. The assessment that there is an immediate threat must include a belief, based on concrete facts, that the procedure with the issuance of a written order would indeed mean that a serious threat to the safety of people or property could not be prevented. At the same time, the severity of the imminent threat must also be assessed - if it cannot be assessed as serious, an oral order cannot be issued.

A search of an electronic device may be ordered and carried out independently or as part of a house search. In this case, the order to search the electronic device is part of the house search order, which may only be carried out on the basis of an order issued at the request of the public prosecutor.

A special case of searching an electronic device without a court order is if the search reveals data that is not related to the criminal offence for which the search was ordered, but rather indicates another criminal offence for which the perpetrator is being prosecuted ex officio. This data is also seized, which is recorded in the minutes and reported to the public prosecutor, who may initiate criminal prosecution. Otherwise, this data is immediately destroyed in the minutes, unless there is another legal reason for taking the data (paragraph nine of Article 219.a of the Criminal Procedure Code). In this case too, the search will only be lawful if the original, initial search is lawful, and the data prima facie indicates another criminal offence. It must be clear from the conduct of the search that the discovery was unexpected (for example, police officers may not abandon the original search).

### 8.3. Execution

Before the seizure and search of an electronic device, the holder shall be served with a search warrant (third paragraph of Article 219a of the ZKP) and shall be required to hand over the device, unless armed resistance is expected or it is necessary for the search to be carried out unexpectedly or in public places (third paragraph of Article 215 in conjunction with the tenth paragraph of Article 219a of the ZKP). By handing over the device, the holder may avoid a more invasive interference with his privacy, especially when the search of the electronic device is carried out as part of a house search.

The owner or user of an electronic device must provide access to the device, which includes both physical access and the submission of encryption keys, passwords and explanations on the use of the device (editorial duty). Otherwise, he may be fined or closed until he complies with the request, but for a maximum of one month (sixth paragraph of Article 219.a in connection with the second paragraph of Article 220 of the ZKP).

The editorial duty does not apply to the alleged perpetrator, to persons who may not be questioned as witnesses (Article 235 of the Criminal Procedure Code), and to persons who have the status of privileged witnesses in the proceedings (Article 236 of the Criminal Procedure Code).

The investigation is carried out by a person with the necessary professional knowledge (eighth paragraph of Article 219.a of the ZKP). Since the ZKP does not stipulate that the investigation is carried out by the police, its implementation can be entrusted to another expert in addition to experts employed by the police (for example, someone who is a permanent sworn expert in computer forensics, although not within the framework of the rules on expertise).

Before an electronic device is searched, the integrity of the original data and its use in further proceedings must be ensured, which is done in accordance with the rules on securing electronic data.

devices (Article 223a of the ZKP; see Section 3.3 of the Special Part). When conducting an investigation, care must be taken to ensure that the rights of other persons are infringed as little as possible, that the secrecy and confidentiality of data are protected, and that disproportionate damage is not caused.

The device owner may only be present during data protection (Article 223a of the ZKP), but not during the actual search of the electronic device.

The result of the investigation is a report containing (eighth paragraph of Article 219.a of the ZKP): – identification of the electronic device that was examined, – date and time of the beginning and end of the investigation or separately for several investigations, if the investigation was not done in one part,

– persons participating and present in the investigation, – the number of the order and the court that issued it, – the method of conducting the investigation, – the findings of the investigation and other important circumstances.