ARTICLE:

ELECTRONIC EVIDENCE IN THE SLOVENE CRIMINAL PROCEDURE ACT

By **Liljana Selinšek, Ph.D**

Introduction

In October 2009, the Slovene legislator adopted an Act Amending the Criminal Procedure Act[1] (CPA-J). With this law, two new articles entered the Criminal Procedure Act: article No. 219.a and article No. 223.a. Both articles regulate basic standards (guidelines) for the collection of electronic evidence for criminal proceedings, and are based on the fact that in the great majority of cases, it is not the electronic device that is crucial, but the data stored in or on it.[2]

As can be noted from the material prepared in the adoption of the CPA-J procedure, the main reason for the legislator's decision on the new articles was the decision of the Constitutional Court No. Up-106/05 of 2 October 2008.[3] In this case, the Constitutional Court decided that reading the content of SMS messages, and searching for and acquiring the data about the most recent telephone calls that were made and those telephone calls that were not answered, are to be treated as the examination of the content and circumstances of the communication. For the police to be able to search the mobile telephone and SIM card, it is necessary to abide by the provisions of article 37 of the Slovene Constitution[4] (one of these conditions is to obtain a court order). However, it has to be stressed that the new articles not only regulate the collection of electronic evidence that interferes with the constitutional right to privacy of communication privacy (such cases are included in decision of the Constitutional Court), but the collection of all data in electronic form that can be important for criminal procedure, irrespective of their nature. So the concept of articles 219.a and 223.a is much broader, as required by the decision of the Constitutional Court.

The provisions of articles 219.a and 223.a of the CPA, in a rather complex and mutually linked way, regulate three procedural activities connected with electronic evidence: (a) the seizure of electronic devices, (b) the preservation of data in electronic form, and (c) the investigation of electronic devices.

Because the regulation was adopted only recently, it is not possible to estimate its efficiency in practice yet, so this article concentrates primarily on a presentation of the provisions in the new articles. In this connection, it is generally important to know that the meaning of the term "electronic device" is a broad one in the Slovene CPA. It is used for electronic devices as well as devices connected to an electronic device, and also for electronic data holders. In this respect, section 219.a paragraph 1 of the CPA is forward looking, because it provides as follows:

> (1) Preiskava elektronskih in z njo povezanih naprav ter nosilcev elektronskih podatkov (elektronska naprava), kot so telefon, telefaks, računalnik, disketa, optični mediji in spominske kartice, se zaradi pridobitve podatkov v elektronski obliki lahko opravi, če so podani utemeljeni razlogi za sum, da je bilo storjeno kaznivo dejanje in je podana verjetnost, da elektronska naprava vsebuje elektronske podatke:

[1] *The Act Amending the Criminal Procedure Act was published in Official Gazette of Republic of Slovenia, No. 77/2009.*

[2] *See Matej Kovačič, Komentar določb novele Zakona o kazenskem postopku (ZKP-J), ki opredeljujejo nekatere posege v komunikacijsko zasebnost (2009), p. 1 [Commentary of CPA-J provisions that are regulating some encroachments upon communication privacy]. Available on-line at http://hr-cjpc.si/pravokator/index.php/2009/10/21/novela-zakona-o-kazenskem-postopku-posegi-v-komunikacijsko-zasebnost/.*

[3] *A case note of this decision of the Slovene Constitutional Court with a commentary is provided in the Digital Evidence and Electronic Signature Law Review 6 (2009), pp. 287 – 289.*

[4] *Article 37 of Constitution of Republic of Slovenia provides for the protection of the privacy of correspondence and other means of communication:*
"The privacy of correspondence and other means of communication shall be guaranteed.
Only a law may prescribe that on the basis of a court order the protection of the privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a set time where such is necessary for the institution or course of criminal proceedings or for reasons of national security."

– na podlagi katerih je mogoče osumljenca ali obdolženca identificirati, odkriti ali prijeti ali odkriti sledove kaznivega dejanja, ki so pomembni za kazenski postopek, ali

– ki jih je mogoče uporabiti kot dokaz v kazenskem postopku.

(1) The investigation of electronic and related devices, and electronic media (electronic device), such as telephone, facsimile, computer, floppy disk, optical media and memory cards, the purpose of obtaining information in electronic form can be made if there are reasonable grounds for suspicion that the offense was committed and there is a likelihood that the electronic device includes electronic data:

- on the basis of which it is possible to identify a suspect or accused, arrested or discover or detect traces of criminal acts that are relevant to criminal proceedings, or

- which can be used as evidence in criminal proceedings.

This list is not closed, so other devices can be listed as an electronic device and will therefore be subject to the provisions of the additional articles.

The seizure of electronic devices and the preservation of data in electronic form

The provisions on the seizure[5] of electronic devices are closely connected with the rules for the preservation of data in electronic form. In fact the only provision on the seizure of electronic devices is the first paragraph of article 223.a, and it does not regulate the way in which an electronic device should be seized, but sets out the further steps where an electronic device is seized because of investigation of its content. If the electronic device is seized as the result of an investigation, there are two possible ways of preserving the data:

a) the electronic data should be saved on another proper data holder in a way that their identity and integrity is preserved and they can be used in further procedure, or

b) the identical copy of the whole data holder should be made and the integrity of this copy should be assured.

If neither of these operations is possible, section 223.a paragraph 1 provides that the electronic device should be sealed as a whole or, if possible, only that part of the device that probably contains the data to be search should be sealed.

During the process of preserving the data, the hash value must be written down in the minutes that have to be carefully kept during the time the data is being preserved, or some other proper way has to be used to enable subsequent checking of the identity and integrity of the preserved data.[6]

The owner, user, administrator or guardian of the electronic device or the person that has access to the device is obliged, on the demand of the authority that has seized the device, to do everything necessary that he or she is able to do to prevent the data from being destroyed, altered or hidden. If they do not do so, he or she can be punished by a fine[7] or even imprisoned,[8] except if he or she is a suspect, defendant or the person that is not allowed to be called as a witness, or if he or she decided not to appear as a witness in accordance with the provisions of the CPA.[9]

The owner of the device has to be invited to be present him or herself, with his or her representative, defence lawyer or expert of his or her choice, at the place that the preservation of the data is to take place. If he or she does not respond to the invitation, or if he or she is absent or unknown, it is possible to undertake the preservation of the data and produce an identical copy of the data in his or her absence.[10] However, the seizure and preservation of the data must be carried out in a way that any encroachment upon the rights of people that are not suspects or defendants is minimal, and data that is of a secret or confidential nature is protected; and in the phase of seizure and preservation

[5] *The provisions on the seizure of electronic devices are of a special nature in comparison to the general provisions in the CPA regulating seizure of (all other kinds of) objects. The provisions on the seizure of electronic devices are of special nature in comparison with general provisions, including seizure of all other objects (i.e. objects different from electronic devices). In Slovene legal theory there are two main types of provisions: general and special. If there are conditions for the use of special provisions, the general one is not used.*

[6] *Section 223.a (paragraph 5) CPA.*

[7] *The fine should be at minimum one fifth of the average net salary in the Republic of Slovenia and not more than three times of the salary. The average net salary is published every month. In March 2010, it was 967,32 Euros (so persons who refused to cooperate with the investigation of an electronic device could be fined of between 193,46 Euros and 2901,96 Euros in March 2010).*

[8] *The person can be held without charge until he or she provides the information (decryption keys, passwords or explanations), but they cannot be held for longer that one month.*

[9] *See 223.a (paragraph 3) CPA.*

[10] *See 223.a (paragraph 4) CPA.*

of data, the authorities are not to cause any disproportionate damage that would prevent the owner or user from being able to use the electronic device during the time when it is the object of seizure.[11]

As in the case of the investigation of an electronic device, only a properly qualified person can be instructed to preserve the data. There are a number of questions that have not been determined regarding who this person can be in Slovenia, and these questions arise on many different levels.[12] As for the regulation, it is not necessary that the preservation of the data in electronic form is performed by a police expert.[13] The legal term "properly qualified person" is only meant to indicate that the person must have enough knowledge for this work, regardless of the sector he or she is part of.[14] The legal provisions are also broad enough to allow the police to employ the services of a digital evidence specialist from the private sector as and when they are needed.

The provisions of article 223.a provide rules that regulate the retention of devices and data that are seized.[15] The rules are the following:

the *electronic device* should be kept until the data are preserved in a way that their identity and integrity is assured, but not more than three months after it was seized. However, if copying the data is not possible, the electronic device or the part that is carrying the searched data should be kept until this is needed for the procedure, but not more than six months, except if the electronic device that was seized was used to commit a criminal offence or the electronic device itself is the evidence in the criminal procedure,

the *copies of seized data* have to be kept until this is needed for the procedure. However, if the data are not connected with the criminal prosecution and there is no other legal reason for their capture, they should be extracted from the court record if this is possible, and destroyed.[16]

The investigation of an electronic device

After the seizure of an electronic device and the preservation of any data stored in the device, the investigation of the device should be performed with the aim of establishing if there is any digital evidence connected to the criminal offence that is the object of investigation. This is a different phase from the seizure and preservation of the data. The investigation phase of aims to obtain an insight into the content stored on the electronic device.

As previously mentioned, under the provisions of article 219.a (paragraph 1) of the Slovene criminal procedure law, the investigation of electronic devices and devices connected to them, as well as the investigation of electronic data holders, can be performed for the purpose of acquiring data in electronic form providing there is a *reasonable ground for suspicion* that a certain criminal offence was committed and it is probable that the electronic device contains electronic data:

a) that would enable the investigating authorities to identify, find or arrest the suspect or the defendant or that would enable the investigating authorities to find the traces of criminal offence that are important for criminal procedure, or

b) that can be used as the evidence in criminal procedure.

There are two possible legal grounds for this investigation.[17] The first one is where *written consent* is given to the police in advance by the owner and known and reachable users of electronic device that have a reasonable expectation of privacy in relation to the device (for instance, if it is a mobile telephone, it is probable that many of the people who made calls to the telephone are innocent of any offence that is under investigation). This possibility is used especially in cases where a device owned by the victim of criminal offence is searched for electronic evidence,[18] because

[11] *See 223.a (paragraph 6) CPA.*

[12] *Janja Bernard, Liljana Selinšek, Benjamin Lesjak and Janko Šavnik, Digitalna forenzika v kazenskih postopkih [Digital Forensics in Criminal Procedures] (Ljubljana, GV založba, 2008), pp. 27 – 29.*

[13] *But there are also opinions that this expert should necessarily be the part of the police forces (i.e. a police investigator). Andreja Lang, Preiskovanje komunikacijske in elektronske zasebnosti po ZKP-J [Investigation of communication and electronic privacy], (Zbornik 2009), konferenca kazenskega prava in kriminologije, Ljubljana, GV založba, p. 180.*

[14] *For more about this topic, see Liljana Selinšek, Ravnanje z elektronskimi napravami po ZKP-J: zgolj policija ali tudi drugi državni organi? [Dealing with electronic devices acording to CPA-J: only the police or also other state authorities?], Pravna praksa, 3-4/2010, pp. 18 – 19.*

[15] *See 223.a (paragraphs 7 and 8) CPA.*

[16] *This destruction has to be notified to the investigating judge, the state prosecutor and the owner of the electronic device within eight days.*

[17] *Both are included in 219.a (paragraph 2) CPA.*

[18] *Matej Kovačič, Komentar določb novele Zakona o kazenskem postopku (ZKP-J), ki opredeljujejo nekatere posege v komunikacijsko zasebnost [Commentary of CPA-J provisions that are regulating some encroachments upon communication privacy], (2009) p. 2. Available on-line at http://hr-cjpc.si/pravokator/index.php/2009/10/21/novela-zakona-o-kazenskem-postopku-posegi-v-komunikacijsko-zasebnost/.*

suspects usually do not give consent for the investigation of their electronic device. In cases where there is no written consent, the investigation can be performed only on the basis of a *written court* order issued on the proposal of a state prosecutor.[19]

The prosecutor's proposal and the court order[20] to investigate the electronic device have to contain the following information:[21]

a) the data that enable the identification of the electronic device that is the object of the investigation;

b) an explanation of the reasons for the investigation;

c) a determination of the data the investigators are looking for; and

d) any other important circumstances that support the use of this method of investigation and to determine why it is important.

Exceptionally, if the court order cannot be acquired within the time limit, and if there is *a direct and serious danger for the safety of people and property*, the investigating judge is allowed, on the basis of an oral proposal by a state prosecutor, to order the investigation of the electronic device by means of an oral court order.[22] Where such an oral proposal and oral order is made, the investigation judge is required to prepare an official note for the file. A written court order must be issued 12 hours after the oral order at the latest. Where the police have fulfilled the oral order, but no written court order has been issued, the police are required to destroy or to delete any of the data that was saved or copied. They must also inform the investigating judge, state prosecutor and owner or user of the electronic device (if he or she is known) within eight days that the data has been deleted.[23]

The investigation of the content stored on the electronic device has to be performed in such a way that the integrity of the original data is preserved, and the data can be used in any further procedure. The investigation also has to be performed in such a way that any encroachment upon the rights of the people that are not suspects or defendants is minimal, and any secret or confidential data is protected and no disproportionate damage is done.[24] As already mentioned above, the investigation of an electronic device has to be carried out by expertly qualified person.[25] During the investigation, the minutes (the written record) has to be maintained, and must include the following information:[26]

a) identification of the electronic device that was investigated;

b) the date and time of the beginning and end of the investigation, and if there are further investigations, date and time of each of them, if the investigation was not carried out at one time;

c) the names of the people that cooperate or are present at the investigation;

d) the number of the court order and the court that has issued the order;

e) the way the investigation was performed;

f) the results of the investigation and any other important and relevant circumstances.

An important provision relates to the cooperation of the owner or user of the electronic device. Paragraph 6 of article No. 219.a of the CPA obliges the owner or user of the electronic device to enable the authorities to obtain access to the device, to provide decryption keys or passwords and explanations on how to the use the device that are necessary for the purpose of the investigation. Failing to provide such help to the authorities can lead to a fine or even imprisonment.[27] However, this rule cannot be used against those people

[19] *If the investigation is performed on the basis of a court order, one copy of the order must be handed to the owner or user of the electronic device that is the object of the investigation.*

[20] *If an electronic device investigation is ordered in the court order for a house or personal search, for this part of the order, the above mentioned rules have to be used. In this case, the proposal for a house or personal search has to be given by the state prosecutor. See 219.a (paragraph 4) CPA.*

[21] *See 219.a (paragraph 3) CPA.*

[22] *See 219.a (paragraph 5) CPA.*

[23] *A similar rule is contained in paragraph No. 2 of article 223a CPA. According to this provision, if the electronic device was seized without a court order and a copy was made to preserve the data, but the court failed to issue the order for the investigation within twelve hours in accordance with paragraph 5 of article 219.a of the CPA, or there was no written consent in accordance with paragraph 2 of article 219.a, the police are obliged to destroy the copy and notify this fact to the investigating judge, state prosecutor and owner or user of electronic device if he or she is known, within eight days.*

[24] *See 219.a (paragraph 7) CPA.*

[25] *Because there are no standards (connected with education, working experiences etc.) for the expertly qualified person, it is for the court to decide if the investigation of the electronic device was performed by a person with the appropriate qualifications.*

[26] *See 219.a (paragraph 8) CPA.*

[27] *The rules on fines and imprisonment are the same whether the owner, user, administrator or guardian of the electronic device refuses to answer the demand for immediate action to prevent any possible destruction, alteration or hiding of the data in the seizure and preservation phase.*

who are protected by constitutionally guaranteed privilege against self-incrimination,[28] such as a suspect, defendant and the person that is not allowed to be called as a witness, or the person that decided not to appear as a witness in accordance with the provisions of the CPA.

Within the provisions of article 219.a there is also a rule connected with the *plain view doctrine*, including instructions for dealing with cases where electronic evidence is discovered coincidentally. If during the investigation data are found that are not connected with the criminal offence for which the investigation was ordered, but the data indicates that another criminal offence might have been committed, this data may also be the subject of a seizure. Where this occurs, it has to be noted down in a minute and immediately reported to the state prosecutor in order to start a prosecution. However, if the state prosecutor realizes there is no reason to carry out a criminal prosecution, and there is no other legal reason for the seizure of this data, the data has to be immediately destroyed. The relevant minutes must be retained about the destruction of such data.[29]

The final, but crucial provision, is the rule set out in paragraph 11 of article 219.a of the CPA. If an investigation of an electronic device was carried out without a court order or in the contradiction of a court order, or if it was carried out without the written consent of the owner or user of the electronic device, *the court is not permitted to make its decision based on the investigation minutes and on the data acquired during the investigation*. Where the rules about the legal grounds for the collection of electronic evidence are violated, the data acquired or the electronic evidence observed are not admissible.

Conclusion

The decision of the Slovene legislator to include provisions on the seizure of electronic devices, and the investigation and preservation of electronic data into the Criminal Procedure Act was welcomed in Slovene theory and practice. However, the legal regulation is only the first step in the process of recognizing electronic evidence not only as legally, but also as factually equal to classical forms of evidence.[30] In Slovenia, the lack of properly qualified digital evidence specialists to perform investigations on electronic devices is a serious concern, as is the lack of funds for the equipment (hardware and software) for digital forensic investigations. Besides, it has to be stressed that the amendments to the CPA only cover the legal framework.[31] But there are no rules for the estimation of the probative value of electronic evidence. This is not the problem, because one of the basic principles of Slovene criminal procedure law is the principle of free estimation of evidence.[32] The problem is, however, that judges (and also state prosecutors and other lawyers) in Slovenia do not have any permanent educational programme where they could get at least basic information about the nature of electronic evidence which is crucial for the correct estimation of probative value of this type of evidence. Also, there are no books in the Slovene language that explains that electronic evidence is highly volatile and can easily be modified, often without any traces, so even electronic evidence that is collected legally might not necessarily be of high probative value. The new CPA regulation is only the start, but the major part of the work is still waiting to be done.

Liljana Selinsek is a member of the editorial board and an adviser at the Office of the Information Commissioner of the Republic of Slovenia

[28] *For more about the dilemmas connected with the privilege against self-incrimination in the information age, see Liljana Selinšek, Privilegij zoper samoobtožbo v informacijski dobi [Privilege against self incrimination in information age], Pravna praksa, 28/2009, pp. 11 – 13.*

[29] *See 219.a (paragraph 8) CPA.*

[30] *For a general introduction to the law in Slovenia in English, see the chapter 'Slovenia' by Ana Burgar and Klara Miletič in Stephen Mason, general editor, International Electronic Evidence (British Institute of International and Comparative Law, 2008), pp. 793 – 833.*

[31] *At present, this regulation is adopted only in respect of criminal procedure law, i.e. in Criminal Procedure Act. But there are no similar provisions in the Civil Procedure Act, where electronic evidence also appears. In civil procedure, electronic evidence is used on the basis of the general provision in the Civil Procedure Act, article No. 16.a: "The data in digital form should not be treated as without probative value only because they are in digital form.".*

[32] *According to principle of free estimation of evidence, there are no rules about the way evidence is to be estimated, so the court estimates the probative value of electronic and other kind of evidence free, on its own logical and psychological analyse. Therefore the court is not obliged by any formal rules to estimate evidence in terms of the probative value of the (electronic) evidence. But, as a rule, the estimation of evidence has to be explained in the grounds of the judgement, where the court is obliged to allege precisely and completely which facts are considered as proved or unproved and for what reasons.*

Original text of articles 219.a and 223.a CPA:

219.a člen

(1) Preiskava elektronskih in z njo povezanih naprav ter nosilcev elektronskih podatkov (elektronska naprava), kot so telefon, telefaks, računalnik, disketa, optični mediji in spominske kartice, se zaradi pridobitve podatkov v elektronski obliki lahko opravi, če so podani utemeljeni razlogi za sum, da je bilo storjeno kaznivo dejanje in je podana verjetnost, da elektronska naprava vsebuje elektronske podatke:

– na podlagi katerih je mogoče osumljenca ali obdolženca identificirati, odkriti ali prijeti ali odkriti sledove kaznivega dejanja, ki so pomembni za kazenski postopek, ali

– ki jih je mogoče uporabiti kot dokaz v kazenskem postopku.

(2) Preiskava se opravi na podlagi vnaprejšnje pisne privolitve imetnika ter policiji znanih in dosegljivih uporabnikov elektronske naprave, ki na njej utemeljeno pričakujejo zasebnost (uporabnik), ali na podlagi obrazložene pisne odredbe sodišča, izdane na predlog državnega tožilca. Če se preiskava opravi na podlagi odredbe sodišča, se izvod te odredbe pred začetkom preiskave izroči imetniku oziroma uporabniku elektronske naprave, ki naj se preišče.

(3) Predlog in odredba o preiskavi elektronske naprave morata vsebovati:

– podatke, ki omogočajo identifikacijo elektronske naprave, ki se bo preiskala;

– utemeljitev razlogov za preiskavo;

– opredelitev vsebine podatkov, ki se iščejo;

– druge pomembne okoliščine, ki narekujejo uporabo tega preiskovalnega dejanja in določajo način njegove izvršitve.

(4) Če se preiskava elektronske naprave odredi v odredbi za hišno ali osebno preiskavo, za izdajo tega dela odredbe in njeno izvršitev veljajo pogoji in postopki iz tega člena. V tem primeru tudi predlog za hišno ali osebno preiskavo poda državni tožilec.

(5) Izjemoma, če pisne odredbe ni mogoče pravočasno pridobiti ter če obstaja neposredna in resna nevarnost za varnost ljudi ali premoženja, lahko preiskovalni sodnik na ustni predlog državnega tožilca odredi preiskavo elektronske naprave z ustno odredbo. O predlogu državnega tožilca in odredbi preiskovalni sodnik izdela uradni zaznamek. Pisna odredba mora biti izdana najpozneje v dvanajstih urah po izdaji ustne odredbe, sicer policija, ki je odredbo izvršila, zapisniško uniči ali izbriše shranjene ali kopirane podatke in o tem v osmih dneh obvesti preiskovalnega sodnika, državnega tožilca in imetnika oziroma uporabnika elektronske naprave, če je znan.

(6) Imetnik oziroma uporabnik elektronske naprave mora omogočiti dostop do naprave, predložiti šifrirne ključe oziroma šifrirna gesla in pojasnila o uporabi naprave, ki so potrebna, da se doseže namen preiskave. Če noče tako ravnati, se sme kaznovati oziroma zapreti po določbi drugega odstavka 220. Člena tega zakona, razen če gre za osumljenca ali obdolženca ali osebo, ki ne sme biti zaslišana kot priča (235. člen) ali se je v skladu s tem zakonom odrekla pričevanju (236. člen).

(7) Preiskava se opravi tako, da se ohrani integriteta izvirnih podatkov in možnost njihove uporabe v nadaljnjem postopku. Preiskava mora biti opravljena na način, s katerim se v najmanjši možni meri posega v pravice oseb, ki niso osumljenci ali obdolženci, in varuje tajnost oziroma zaupnost podatkov ter ne povzroča nesorazmerna škoda.

(8) Preiskavo opravi strokovno usposobljena oseba. O preiskavi se napravi zapisnik, ki med drugim obsega:

– identifikacijo elektronske naprave, ki je bila pregledana;

– datum ter uro začetka in konca preiskave oziroma ločeno za več preiskav, če preiskava ni bila opravljena v enem delu;

– morebitne sodelujoče in navzoče osebe pri preiskavi;

– številko odredbe in sodišče, ki jo je izdalo;

– način izvedbe preiskave;

– ugotovitve preiskave in druge pomembne okoliščine.

(9) Če se pri preiskavi najdejo podatki, ki niso v zvezi s kaznivim dejanjem, zaradi katerega je bila preiskava odrejena, temveč kažejo na drugo kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti, se zasežejo tudi ti. To se navede v zapisnik in takoj sporoči državnemu tožilcu, da začne kazenski pregon. Ti podatki pa se takoj uničijo, če državni tožilec spozna, da ni razloga za kazenski pregon in tudi ne kakšnega drugega zakonskega razloga, da bi se morali podatki vzeti. O uničenju se sestavi zapisnik.

(10) Če v tem členu ni določeno drugače, se za odreditev in izvršitev odredbe o preiskavi elektronske naprave smiselno uporabljajo določbe tretjega in četrtega odstavka 215. člena ter četrtega, petega in sedmega odstavka 216. člena tega zakona.

(11) âe je bila preiskava elektronske naprave opravljena brez odredbe sodišča ali v nasprotju z njo ali brez pisne privolitve iz drugega odstavka tega člena, sodišče svoje odločbe ne sme opreti na zapisnik o preiskavi in na tako pridobljene podatke.

223.a člen

(1) Če se zaseže elektronska naprava (prvi odstavek 219.a člena) zaradi oprave preiskave, se podatki v elektronski obliki zavarujejo tako, da se shranijo na drug ustrezen nosilec podatkov na način, da se ohrani istovetnost in integriteta podatkov ter možnost njihove uporabe v nadaljnjem postopku ali se izdela istovetna kopija celotnega nosilca podatkov, pri čemer se zagotovi integriteta kopije teh podatkov. Če to ni mogoče, se elektronska naprava zapečati, če je mogoče, pa samo tisti del elektronske naprave, ki naj bi vseboval iskane podatke.

(2) Če je bila elektronska naprava zasežena brez odredbe sodišča in je bila zaradi zavarovanja podatkov izdelana njihova kopija, vendar sodišče v dvanajstih urah ni izdalo odredbe za preiskavo po petem odstavku 219.a člena tega zakona oziroma ni bila dana privolitev po drugem odstavku 219.a člena tega zakona, policija zapisniško trajno uniči izdelano kopijo in o tem v osmih dneh pisno obvesti preiskovalnega sodnika, državnega tožilca in imetnika oziroma uporabnika elektronske naprave, če je znan.

(3) Imetnik, uporabnik, upravljavec ali skrbnik elektronske naprave oziroma tisti, ki ima do nje dostop, mora na zahtevo organa, ki jo je zasegel, takoj ukreniti, kar je potrebno in je v njegovi moči, da se onemogoči uničenje, spreminjanje ali prikrivanje podatkov. âe noče tako ravnati, se sme kaznovati oziroma zapreti po določbi drugega odstavka 220. člena tega zakona, razen če gre za osumljenca, obdolženca ali osebo, ki ne sme biti zaslišana kot priča (235. člen) ali se je v skladu s tem zakonom odrekla pričevanju (236. člen).

(4) Imetnika naprave se povabi, naj bo sam, njegov zastopnik, odvetnik ali strokovnjak navzoč pri zavarovanju podatkov po prvem odstavku tega člena. âe se ne odzove vabilu, če je odsoten ali če ni znan, se zavarovanje podatkov in izdelava istovetne kopije opravi v njegovi nenavzočnosti. Zavarovanje podatkov opravi ustrezno usposobljena oseba.

(5) Pri zavarovanju podatkov se v zapisnik zapiše tudi kontrolna vrednost, oziroma se na drug ustrezen način v zapisniku zagotovi možnost naknadnega preverjanja istovetnosti in integritete zavarovanih podatkov. Izvod zapisnika se izroči osebi iz prejšnjega odstavka, ki je bila navzoča pri zavarovanju podatkov.

(6) Zaseg in zavarovanje podatkov morata biti opravljena na način, s katerim se v najmanjši možni meri posega v pravice oseb, ki niso osumljenci ali obdolženci, in varuje tajnost oziroma zaupnost podatkov ter se ne povzroča nesorazmerna škoda zaradi nezmožnosti uporabe elektronske naprave.

(7) Kopije zaseženih podatkov se hranijo, dokler je to potrebno za postopek. Elektronska naprava se hrani, dokler podatki niso shranjeni na način, ki zagotovi istovetnost in integriteto zaseženih podatkov, vendar ne več kakor tri mesece od dneva pridobitve. âe izdelava takšne kopije podatkov ni mogoča, se elektronska naprava ali del elektronske naprave, ki vsebuje iskane podatke, hrani, dokler je to potrebno za postopek, vendar ne več kakor šest mesecev od dneva pridobitve, razen če je bila zasežena elektronska naprava uporabljena za izvršitev kaznivega dejanja oziroma je sama elektronska naprava dokaz v kazenskem postopku.

(8) Kopije podatkov, pridobljene v skladu z določbami tega člena, ki se ne nanašajo na kazenski pregon in za katere ni kakšnega drugega zakonskega razloga, da bi se smeli hraniti (498. člen), se izločijo iz spisa, če je to mogoče in se zapisniško uničijo, o čemer se v osmih dneh obvestijo preiskovalni sodnik, državni tožilec in imetnik elektronske naprave.

Unofficial translation into English

Article 219.a

(1) The investigation of electronic devices and devices connected to them as well as the investigation of electronic data holders (further on »electronic device«), such as telephone, fax, computer, floppy disk, optical media and memory cards, can be done for the purpose of acquiring data in electronic form, if there is reasonable ground for suspicion that a criminal offence was committed and it is probable that the electronic device contains electronic data:

- that would enable the identification, finding or arrest of the suspect or the defendant or that would help to find the traces of criminal offence that are important for criminal procedure, or
- that can be used as the evidence in criminal procedure.

(2) The investigation can be performed on the basis of written consent given to the police in advance by the owner and known and reachable users of the electronic device that have a reasonable expectation of privacy on the device, or on the basis of a written court order issued on the proposal of a state prosecutor. If the investigation is performed on the basis of a court order, one copy of the order has to be handed to the owner or user of the electronic device that is the object of the investigation.

(3) The proposal and the court order on electronic device investigation have to contain:

- the data that enable the identification of the electronic device that is the object of the investigation;
- an explanation of the reasons for the investigation;
- a determination of the data the investigators are looking for; and
- other important circumstances that allow the use of this investigation method and determine how it is to be performed.

(4) If the investigation of an electronic device is ordered in the court order for the search of a house or a personal search, for this part of the order the conditions from this article are valid. In such a case, the proposal for a house or personal search has also to be given by the state prosecutor.

(5) Exceptionally, if the court order can not be acquired on time and if there is a direct and serious danger for the safety of people and property, the investigating judge is allowed, on the basis of the oral proposal of the state prosecutor, to order the investigation of an electronic device by oral court order. The investigation judge has to write official note about this oral proposal and oral order. The written court order must be issued 12 hours after the oral order at the latest, otherwise the police that fulfilled the order must destroy or delete any saved or copied data and inform, within 8 days, the investigating judge, state prosecutor and owner or user of the electronic device if he or she is known about this fact.

(6) The owner or user of the electronic device is obliged to enable access to the device, to provide decryption keys or passwords and explanations on the use of the device that are needed for the purpose of the investigation. If they fail to provide this information, he or she can be punished or imprisoned according to the second paragraph of article 200 of this act, except if he or she is a suspect, defendant or the person that is not allowed to be called as a witness (article 235) or if he or she decided not to appear as witness according to this act (article 236).

(7) The investigation has to be performed in a way that the integrity of the original data is preserved and the data can be used in further procedure. The investigation has to be performed in a way that encroachment upon the rights of the people that are not suspects or defendants is minimal, and data of a secret or confidential nature is protected and no disproportionate damage is done.

(8) The investigation has to be carried out by an

expertly qualified person. During the investigation the minutes (i.e. the written record) has to be kept that includes:

- identification of the electronic device that was investigated;
- date and hour of investigation beginning and end of the investigation, and if there are more separate investigations, the date and hour of each of them, if the investigation was not carried out at one time;
- the names of the people that eventually cooperate or are present at the investigation;
- number of the court order and the court that issued the order;
- the way the investigation was performed;
- results of investigation and other important circumstances.

(9) If during the investigation data are found that are not connected with the criminal offence for which the investigation was ordered but indicate another criminal offence that is prosecuted ex officio, these data may also be the object of a seizure. This has to be noted down in the minutes and immediately reported to the state prosecutor to start the prosecution. However, if the state prosecutor realizes there is no reason for a criminal prosecution and also no other legal reason for the seizure of this data, the data have to be immediately destroyed. The minutes have to be kept about the destruction of the data.

(10) If there is no other provision in this article, for the ordering and executing of a court order for the investigation of an electronic device, the third and fourth paragraph of article 215, and fourth, fifth and seventh paragraph of article 216 have to be used.

(11) If the investigation of an electronic device was carried out without a court order or in contradiction of a court order, or if it was carried out without written consent from the second paragraph of this article, the court is not allowed to leave its decision on the investigation minutes and on the data acquired during the investigation.

Article 223.a

(1) If an electronic device is seized (first paragraph of article 219.a) for the needs of the investigation, the electronic data have to be secured and saved on another proper data holder in a way that their identity and integrity is preserved and they can also be used in further procedure, or the identical copy of the whole data holder is performed and the integrity of this copy is assured. If this is not possible, the electronic device should be sealed, and if possible only the part of the device that probably contains the searched data should be sealed.

(2) If the electronic device was seized without a court order and the copy was made for the purpose of ensuring the data is available, and the court did not issue an order for the investigation in 12 hours in accordance with the fifth paragraph of article 219.a of this act, or there was no written consent in accordance with the second paragraph of article 219.a, the police are obliged to destroy the copy and notify this fact to the investigating judge, state prosecutor and owner or user of electronic device if he or she is known, within 8 days.

(3) The owner, user, administrator or guardian of the electronic device or the person that has access to the device is obliged, on the demand of the authority that seized the device, immediately to do everything necessary that he or she can do to prevent the possible destruction, changing or hiding the data. If not, he or she can be punished or imprisoned in accordance with the second paragraph of article 200 of this act, except if he or she is a suspect, defendant or the person that is not allowed to be called as a witness (article 235) or if he or she decided not to appear as witness according to this act (article 236).

(4) The owner of the device has to be invited to be present himself, or by his representative, defence lawyer or expert of his choice, when the data is copied according to the first paragraph of this article. If he does not respond to the invitation, or if he is absent or unknown, the data is copied in his absence. The data has to be copied out by a properly qualified person.

(5) In the process of copying the data, the hash value has to be written down in the minutes, or some other

proper way has to be used to assure the possibility of the subsequent checking of the identity and integrity of the data. The issue of the minutes is given to the person from former paragraph that was present at the copying of the data.

(6) The seizure and copying of the data has to be carried out in a way that any encroachment upon the rights of the people that are not suspects or defendants is minimal, and any data of a secret or confidential nature is protected and no disproportionate damage is caused due to the inability of device to be used is done.

(7) The copies of the seized data have to be kept until it is needed for the procedure. The electronic device is kept until the data is preserved in a way that their identity and integrity is assured, but not more than three months after it was seized. If it is not possible to copy the data, the electronic device or the part that is carrying the searched data is kept until it is needed for the procedure, but not more than six months, except if the seized electronic device was used for the commitment of the criminal offence or the electronic device itself is the evidence in the criminal procedure.

(8) Copies of the data, acquired in accordance with this article, that are not connected with the criminal prosecution and there is no other legal reason for their capture (article 498) are extracted from the court record if this is possible, and have to be destroyed. The investigating judge, state prosecutor and owner of the electronic device owner have to be informed in due time within 8 days of this fact.

