ARTICLE:

Criminal procedure and digital evidence in Estonia

By **Eneli Laurits**

Introduction

The Estonian Code of Criminal Procedure (CCP) is now under renewal, since criminal procedure is subject to a revision that is planned to be finished by the year 2020.[1] The most significant reform yet implemented to the Estonian criminal procedural law took place in 2004 when the current CCP came into force (KrMS – the Estonian abbreviation).[2] Among other things, the revision will consider the possibility of making criminal proceedings fully digital in Estonia. The taking and use of evidence in digital form in judicial proceedings also constitutes a part of digital criminal proceedings. Digital evidence is increasingly taken in criminal proceedings, but since the current law does not provide for specific rules of procedure or the principles of taking such evidence, the provisions on the taking and investigation of conventional evidence also remain the basis for digital evidence. There is no definition of digital evidence as a specific type of evidence. One of the aims of the revision is to analyse how and to what extent the provisions concerning digital evidence should be specified in the Estonian criminal procedural law.[3]

The Estonian Code of Criminal Procedure and digital evidence

Section 63 of the CCP stipulates that evidence means the statements of a suspect, the accused, the victim, the testimony of a witness, an expert's report, the statements given by an expert upon provision of explanations concerning the expert's report, physical evidence, reports on investigative activities, minutes of court sessions and reports on surveillance activities, and other documents, photographs, films or other data recordings. Generally speaking, the types of evidence only specified in subsection 63(1) of the CCP (called strict evidence) can be used in criminal proceedings for the reason of proof. Evidence that is not listed in subsection (1) of section 63 may be used in order to prove the facts relating to a criminal proceeding (free evidence, 63 (2)) but not for the reason of proof (for example following the time-limits of proceedings). Reason of proof is stated in section 62. The facts relating to a subject of proof are:

> (1) the time, place and manner of commission of the criminal offence and other facts relating to the criminal offence;
>
> (2) the necessary elements of the criminal offence;
>
> (3) the guilt of the person who committed the criminal offence;
>
> (4) information describing the person who committed the criminal offence, and other circumstances affecting the liability of the person.

The Supreme Court has found that the system of proof suggests a clear differentiation between various admissible types of evidence as well as between various sources of evidence.[4]

The Estonian legislature has specified admissible forms of evidence in criminal proceedings. The above provision (63(1)) is the only provision specifying the types of evidence in the CCP. There is no separate reference nor special procedure prescribed in the general conditions for proof and the taking of evidence. The provisions are as follows:

> CCP § 64. General conditions for taking of evidence
>
> (1) Evidence shall be taken in a manner which is not prejudicial to the honour and dignity of the persons participating in the taking of the evidence, does not endanger their life or health or cause unjustified proprietary

[1] A number of provisions are to be adjusted in the course of the revision of Estonian criminal procedure law, and there is just a small part concerning digital evidence. Although the revision is to be completed by the year 2020, it does not mean that the planned alterations will come into force.
[2] Code of Criminal Procedure. Available at https://www.riigiteataja.ee/en/eli/531052016001/consolide.
[3] Terms of reference of the revision of criminal procedural law (2015), clause 9. Available at http://www.just.ee/sites/www.just.ee/files/kriminaalmenetluse_revisjoni_lahteulesanne.pdf.
[4] RKKKo 3-1-1-142-05, clause 10. Available at http://www.nc.ee/?id=11&tekst=222485753.

damage. Evidence shall not be taken by torturing a person or using violence against him or her in any other manner or by means affecting a person's memory capacity or degrading his or her human dignity.

(2) If it is necessary to undress a person in the course of a search, physical examination or taking of comparative samples, the official of the investigative body, the prosecutor and the participants in the procedural act, except health care professionals and forensic pathologists shall be of the same sex as the person.

(3) If technical equipment is used in the course of taking of evidence, the participants in the procedural act shall be notified thereof in advance and the objective of using the technical equipment shall be explained to them.

(4) [Repealed - RT I, 23.02.2011, 1 - entry into force 01.09.2011]

(5) If necessary, participants in a procedural act shall be warned that disclosure of information relating to pre-trial proceedings is prohibited in accordance with § 214 of this Code.

(6) The taking of evidence by surveillance activities is regulated by Chapter 31 of this Code.

The types of evidence specified in the CCP are described in general terms, so that it has been possible to submit digital evidence into legal proceedings on the basis of this provision.[5] At the same time, discussions over the necessity of a special procedure and specific provisions for digital evidence have been held for some time in the Estonian legal landscape. For example, the Chancellor of Justice has offered an opinion that, taking into account the widespread use of electronic communications, and the extent of fundamental rights' violations caused by disclosure of information contained in electronic data media, it would be appropriate to consider if more precise regulations (accompanied by necessary procedural safeguards) are capable of ensuring the better protection of fundamental rights and freedoms.[6] The Bar Association has also found that even now, electronic data taken during searches are being used as evidence in many of criminal cases, and the importance of such evidence is increasing. In the view of the Bar Association, it is reasonable to separately regulate the obtaining of digital evidence and its use in criminal proceedings. The use of the provisions dealing with conventional evidence to include digital evidence cannot provide for the procedural rights of persons, nor the admissibility, reliability and verifiability of such evidence.[7] The audit analysis for the revision of the CCP indicates that, based on the provisions of the CCP, it might be problematic to treat some types of evidence that are specific and rarely directly used in practice as proofs. This includes the types of evidence described in the relevant provisions, such as physical evidence, other documents and other data recordings that seem to imply the information is stored on data media. However, the digital information transmitted between various devices might also contain evidentiary information to be collected online.[8]

The taking of digital evidence is performed on the basis of the CCP by means of either public investigative measures or surveillance activities conducted secretly from a suspect. In both cases, data are collected and executed pursuant to the existing procedural order. But the CCP only refers to the taking of conventional evidence. This article aims to sum up the most common activities within which digital evidence might be taken, highlighting the potential problems of interest to the legislature when elaborating specific regulations for digital evidence.

Public investigative measures

The most frequent public investigative measures are a search and an inspection, which are set out below:

[5] The Supreme Court has consistently accepted as evidence both SMS messages and e-mail correspondence, but, recordings of private conversations are assessed by the Supreme Court as an information recording as provided for in subsection 63 (1) of the CCP.

[6] The Chancellor of Justice's opinion of 05.12.2012 concerning the CCP and a draft law on alterations made to other laws (295 SE). Available at http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=52727c38-5c97-433d-bc25-eda7af8db244& , clause 27.

[7] The Bar Association's opinion of 14.01.2013 concerning the CCP and a draft law on alterations made to other laws (295 SE). Available at http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=4fe1744a-f345-4fbc-98e2-05f66621c965&, p 10.

[8] J. Tehver, *Analysis Ensuring the Use of Digital Evidence* (2016), p 2. Available at http://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf.

> § 83. Objective of inspection and objects of inspection
>
> (1) The objective of an inspection is to collect information necessary for the adjudication of a criminal matter, detect the evidentiary traces of the criminal offence and confiscate objects which can be used as physical evidence.
>
> (2) The objects of inspection are:
>
> 1) a scene of events;
>
> 2) a body;
>
> 3) a document, any other object or physical evidence;
>
> 4) in the case of physical examination, the person and the postal or telegraphic item.
>
> (3) If the explanations of a suspect, accused, witness, qualified person or victim help to ensure the thoroughness, comprehensiveness and objectivity of the inspection, such person shall be asked to be present at the inspection.

The provisions on a search have been established, are applicable and presume a single-step procedure, i.e., looking for physical evidence. A search is generally limited in both time and physical space. Also, the Code of Criminal Procedure (CCP) clearly relates a search to a particular physical location and physical objects: the objective of a search is to find an object to be confiscated or used as physical evidence, a document, a thing or a person necessary for the adjudication of a criminal matter, property to be seized for the purpose of compensation for damage caused by a criminal offence or for confiscation, or a body, or to apprehend a fugitive in a building, room, vehicle or enclosed area. When the investigation authorities look for digital evidence, dealing with it has been solved in a simple manner: a data medium (usually initially with the casing, i.e., the computer) is seized in the course of a search, and the search for digital evidence will be executed in the form of an inspection or an expert assessment.[9]

The CCP treats the search of a data medium as an 'inspection', and the legislature has so far not found it necessary to afford greater protection of fundamental rights in respect of personal information held electronically. As prescribed in the procedural rules, an inspection is not limited in time. An investigative measure can be performed as long as a body conducting the proceedings deems it necessary, however the terms and the course of an investigative activity must be stated in an inspection report. An electronic data medium usually contains so much personal information (and not only on the possible suspect, but also on family members, etc.) that a search of such information should be regarded as a major infringement of the person's privacy.[10] During an inspection, a body conducting the proceedings can look through the data medium, which could be relevant to the proceedings, essentially during an unlimited period of time and for unlimited number of times. Moreover, a body conducting proceedings does not even have to know what in particular is to be found. A body conducting proceedings can just look for something that will be useful, provided it has enough time. When searching a physical space, such as in the course of the search of a domestic dwelling, the body conducting the proceedings is not permitted to search beyond the time limit set down.[11]

Prior to the commencing of an inspection, a body conducting proceedings has no obligation to submit or to substantiate the reasons for the performance of an investigative measure. After conducting an inspection, the investigator has to set out those findings in an inspection report that are important in the view of criminal proceedings. The investigator may conduct this kind of inspection for as long as is necessary, and they may look through everything. The investigator does not have to specify what she is looking for or where she has looked into, only the findings are finally set out in the report. However, in case of a search, a body conducting proceedings has to specify precisely what is to be found, and to obtain a respective permission from a prosecutor or a court, while an inspection remains within a discretional power of a body conducting the proceedings. Although an infringement of the person's fundamental rights during the examination of a data medium is severe, and it can be compared to a search of the person's

[9] E. Laurits, 'Some problems encountered in computer system searches', *Yearbook of Estonian Courts* (2015), pp 136-137. English version available at http://www.riigikohus.ee/vfs/2071/Riigikohtu_aastaraamat_eng_veebi.pdf.

[10] Ortiz Pradillo, 'Fighting Against Cybercrime in Europe: The Admissibility of Remote Searches in Spain', *European Journal of Crime, Criminal Law and Criminal Justice*, 19 (2011), clause 383.

[11] E. Laurits, 'Some problems encountered in computer system searches', *Yearbook of Estonian Courts* (2015), p137. English version available at http://www.riigikohus.ee/vfs/2071/Riigikohtu_aastaraamat_eng_veebi.pdf.

place of residence, the Estonian legislature has not so far deemed it necessary to set forth a special regulation to that effect.

In addition to which, there are provisions stipulating that evidence seized during a search of a physical place that comes under the 'plain view' exception. Digital evidence is subject to the plain view exception, however, is not regulated. For example, while examining a data medium, a body conducting proceedings may discover abusive images of children, documents referring to an economic criminal offence, and pictures or videos referring to any number of criminal offences. Although investigators may see and discover during a physical search the plain view exception relevant to another criminal offence (for example, abusive images of children), such evidence is regularly found during a subsequent examination of digital media. The provisions of the CCP on inspections do not restrict the activities of bodies conducting proceedings in the performance of an inspection that could result in a finding of incriminating materials that were not expected to be found in the first place.[12]

The audit analysis points out that the searching of the content of a data medium is regarded as an inspection that needs to be separately regulated in a manner similar to a physical search against a court's permission. What is fully justified is the conclusion that searching a data medium means a severe infringement of the person's privacy.[13] It is indisputable that many people record a major part of their life as digital information to an accessible server environment of a data media or through devices used by them. Arguably, they subjectively expect that their privacy is to be respected.

The problems concerning the examination of a data medium is but one part of the problem. The CCP does not stipulate a computer system as a place to be searched that affords a body conducting proceedings an opportunity to move beyond the physical space of the hard disk during the search and to record data, for example, if the evidence is in an e-mail box. The CCP does not stipulate the possibility for a body conducting proceedings to extend the search of a computer system to other computer systems in the territory of Estonia, as provided in the order specified in article 19(2) of the Convention on Cybercrime. However, it must be mentioned that searches can be continued on Estonian servers once the investigators have obtained access to a computer system. The problem is, that in the majority of cases, a cross-border approach is essential. There is no regulation for the taking of data across borders.[14]

Practitioners specialising in criminal proceedings have repeatedly given their opinions orally – primarily in workshops – about the necessity of a regulation for the search of a computer system. At present, cross-border searches of computer systems are performed either as an inspection or by a surveillance activity. The existing norms and principles are being adjusted to handle such situations when, for example, upon apprehension, a suspect has a computer or a smartphone unprotected with a password, and it is possible to obtain and to look through the information about the data stored, for example, in the cloud or in an e-mail box (which are not on the Estonian servers). Even when prosecutors approach the court on their own initiative, and by pointing out an obvious similarity between the search of a computer system and the search of a physical space to obtain permission from the court, preliminary investigation judges have so far found that such permission is not needed.[15]

The taking of evidence by surveillance

In addition to public investigative measures, evidence can be taken in criminal proceedings secretly from a data subject by means of surveillance activities. The Estonian Supreme Court has found that where a person is not aware of being subjected to surveillance, it can infringe their fundamental rights more severely as compared with any other investigative measure. From the evidentiary point of view, the secrecy of a surveillance activity means that an accused will become aware of the evidence only after a specific

[12] E. Laurits, 'Some problems encountered in computer system searches', *Yearbook of Estonian Courts* (2015), pp 136-139. English version available at http://www.riigikohus.ee/vfs/2071/Riigikohtu_aastaraamat_eng_veebi.pdf.

[13] J. Tehver, *Analysis Ensuring the Use of Digital Evidence* (2016), pp 8-9. Available at http://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf.

[14] In certain circumstances, the police in England & Wales can use evidence from another jurisdiction, for which see Esther George and Stephen Mason, 'Obtaining evidence from mobile devices and the cloud', *Computer and Telecommunications Law Review*, 2015, Volume 21, Issue 8, pp 245 – 252. The position is the same in Denmark: U 2012.2614 H, commentary by Professor Lars Bo Langsted, *Digital Evidence and Electronic Signature Law Review*, 10 (2013), pp 162 – 165.

[15] For example, judgment of the Harju County Court No. 1-15-10001.

activity has been performed.[16] A precondition for the conduct of surveillance activities is that they are permitted if the collection of data by other activities or the taking of evidence by other procedural acts is impossible because of the limit on time; it is especially complicated, or if this may damage the interests of the criminal proceedings.[17] The CCP stipulates the criminal offences in the event of which it is permitted to conduct surveillance activities.[18] A surveillance agency may covertly enter a computer system, covertly watch a person, thing or area, covertly take comparative samples and perform initial examinations, covertly examine a thing and covertly replace it. The information collected through such activities must be, if possible, video recorded, photographed or copied or recorded in another way. It is also permitted to intercept or to covertly observe messages or other information transmitted by the public electronic communications network or where messages are communicated by any other means. Pursuant to the law, a permission granted by a preliminary investigation judge is needed to enter a computer system and to intercept and to covertly observe messages or other information transmitted over the public electronic communications network, whereas it only requires the permission of a prosecutor to covertly examine a thing.

Discussion has taken place in the Estonian legal landscape over the degree of protection of the confidentiality of communications in the digital age. Section 43 of the Constitution of the Republic of Estonia[19] directly speaks of transmitted messages, not of any messages, and proceeding from the Supreme Court also have found that the protection of the confidentiality of communications matters as a protective clause of communications process only and is not meant to protect the confidentiality of communication as it is transmitted. Consider the judgment of the Criminal Chamber of the Supreme Court of 30.06.2014 No.3-1-1-14-14, clause 816. This concept is clarified in clause 817 of the judgement:[20]

> 'The strict protection provided by the Fundamental Law applies with regard to an e-mail letter or a SMS-message as from the moment it is sent until it is received by a recipient, to a telephone conversation at the moment it is being hold and to a postal item as from the moment it is transferred to a post office until it is delivered to an addressee. This circumstance is substantiated by the fact that during the time a message is on the way, i.e. it has left the sender's possession and it has not yet reached a recipient, a message is beyond the person's control and it cannot be protected from third parties. When a message has reached a recipient, a person has a choice either to delete the message or to make it inaccessible to third parties in any other manner. Consequently, no court permission is needed to seize messages which have already reached the recipient, and an appropriate investigative measure under the Fundamental Law to attach them to the criminal case shall be both a search and an inspection.'

Yet not all jurists agree with this narrow interpretation. The issue is whether the confidentiality of messages as stipulated in the Fundamental Law reflects the technology of the 21st century, and whether it is reasonable to provide the protection for messages only at the time of their transmission.[21] One justice of the Supreme Court offered a dissenting opinion regarding the above interpretation.[22] The Supreme Court has found that a permission granted by a prosecutor, and not by a court, is enough to observe, copy data in the person's e-mail box (including when an e-mail box is located on a foreign state's server) and to covertly examine a part of the server where a particular e-mail box is located, because messages are then not being transmitted, but they have already reached a recipient.[23]

[16] Judgment of the Criminal Chamber of the Supreme Court's No. 3-1-1-63-08, clause 13.2. Available at http://www.nc.ee/?id=11&tekst=RK/3-1-1-63-08.
[17] CCP § 126^1.
[18] CCP § 126^2 subsection 2.
[19] English version available at https://www.riigiteataja.ee/en/eli/521052015001/consolide. § 43: everyone has the right to confidentiality of messages sent or received by him or her by post, telegraph, telephone or other commonly used means. Derogations from this right may be made in the cases and pursuant to a procedure provided by law if they are authorised by a court and if they are necessary to prevent a criminal offence, or to ascertain the truth in a criminal case.
[20] Available at http://www.nc.ee/?id=11&tekst=222574833.
[21] U. Lõhmus, 'Once more about messages' confidentiality or what impact the 20th century technology has on the Fundamental Law's interpretations', *Juridica* III/2016, pp 175-183.
[22] The judgment of the Criminal Chamber of the Supreme Court of 20.11.2015 No. 3-1-1-93-15 and the dissenting opinion of Kergandberg J. Available at http://www.riigikohus.ee/?id=11&tekst=222579511.
[23] The judgment of the Criminal Chamber of the Supreme Court of 20.11.2015 No. 3-1-1-93-15, clause 92. Available at http://www.riigikohus.ee/?id=11&tekst=222579511.

Concerning the taking of evidence in a digital form, including data stored in the cloud, the Estonian courts have not discussed the problem of jurisdiction for the taking of evidence and whether it is justified to request such data by way of mutual legal assistance treaty. At present, the discussion revolves around data protection as provided by the Fundamental Law and with permission granted by an authority with whom it has a lawful right to infringe a right. Thus, the Estonian Supreme Court has, in essence confirmed universal jurisdiction.

The Estonian CCP foresees that the evidence taken in a foreign state pursuant to the legislation of such state may be used in a criminal proceeding conducted in Estonia unless the procedural acts performed in order to obtain the evidence are in conflict with the principles of Estonian criminal procedure,[24] and so far it covers evidence from a foreign state by way of a request for legal assistance. However, it is already commonly known that this technique is regretfully not effective for the taking of digital evidence.[25] There are no special provisions in the CCP to this effect, and the courts have not voiced any opinion regarding jurisdiction. The *Advisory Guidelines on IT-Evidence*, prepared on 24.05.2016 by law enforcement agencies, claim that in case of public investigative measures (inspection, search) and covert surveillance, no request for legal assistance is needed for data stored in cloud on foreign states' servers. This is because an action (the copying of data) is performed in the territory of Estonia by an Estonian body conducting proceedings, and the data can be received without physically leaving the territory of Estonia, and Estonia has the jurisdiction to copy the data.[26] A general principle for the territorial and temporal applicability of Estonian criminal procedural law is stipulated in section 3 of the CCP, pursuant to which the criminal procedural law applies in the territory of the Republic of Estonia. This provision is also supported by the fact that in many cases there is a loss of location, and a body conducting proceedings does necessarily know where data are located, and therefore no request for legal assistance can be sent. At the same time, in some cases it is possible to ascertain the location of a server, and this brings up the question whether such an approach violates the state's sovereignty or not. There are no special provisions in the Estonian law concerning jurisdiction upon taking of digital evidence, and there have been no cases brought before the Supreme Court.

Competency to seize digital evidence

The CCP does not stipulate the competencies for a person seizing digital evidence. There are no references in the CCP to the requirements (education or skills) in respect of a person taking evidence. Although the CCP stipulates a difference for taking personal evidence during the hearing of children with the aim of avoiding undue damage to a child, and to other fragile evidence (an obvious similarity to digital evidence might be mentioned in this respect!). So, the CCP stipulates that in particular cases a body conducting proceedings must receive appropriate training to take testimony of a child,[27] whereas it is not stipulated at all what such appropriate training must be for the digital evidence professional. The issue is entirely left to be shaped and defined by practice and the decisions of judges.

It is reasonable to stipulate that digital evidence can only be seized by a person having appropriate training, since it is very easy to alter digital data. Disputes occur regarding the mishandling of digital evidence.[28] Presently, evidence is taken by investigative bodies' officials who are entitled to be involved in the taking of evidence if necessary. It can be either an expert (who does not have to be a body conducting the proceedings), or an IT-expert from the Estonian Forensic Science Institute. A decision over the involvement of an expert is made either by a prosecutor leading the proceedings or by an official of the investigative body, though they is not obliged to do so.

The incompetent taking of digital evidence threatens not only a proceeding, but it may bring about a

[24] CCP § 65.
[25] Mutual legal assistance is a mechanism through which evidence of a criminal proceeding is obtained from another jurisdiction. In December 2014, an assessment was carried out as to the effectiveness of requests for legal assistance. It was concluded that requests for legal assistance are generally ineffective, in particular, when taking digital evidence. The average time for response to such a request is between 6-24 months. Many requests are not responded at all. (*Criminal justice access to data in the cloud: challenges*, discussion paper. prepared by the T-CY Cloud Evidence Group (2015), page 14. Available at http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2015/T-CY(2015)10_CEG%20challenges%20rep_sum_v8.pdf.
[26] The Advisory Guidelines on IT-Evidence (2016) (in the author's possession).
[27] CCP § 70.
[28] L. Selinšek. 'Electronic evidence in the Slovene Criminal Procedure Act', *Digital Evidence and Electronic Signature Law Review*, 7 (2010), pp 77 – 86.

wrongful court judgement.[29] Mistakes made during the taking of digital evidence are not necessarily noticed later on and in addition, since this is time-sensitive evidence, it is not necessarily possible to take additional essential evidence at a later time when mistakes have been already made.

The audit analysis has not touched upon this subject, though it is important for several reasons. First, it is important for ensuring the quality of evidence on a national level. It is unacceptable when a body conducting proceedings depend on the discretionary power of a senior person with no qualifications, where in reality, evidence may be seized by officials whose lack of competence fatally changes evidence, or who are not capable of explaining to the court how they have taken the evidence and why they have done it one way and not another.

Second, since the taking of digital evidence is highly important for the investigation of serious crimes, it is necessary to provide for the conformity of taking of evidence in Estonia to a level and competence similar to a commonly recognised one when providing a legal assistance to another state. Finally, it lies solely within the competence of an agency to decide whether to establish special police units (to investigate cybercrimes for instance).

Issues brought up in the audit analysis in respect of digital evidence

The issues brought up as a result of initial analysis in the audit report need to be further analysed, for example, by creating an evidentiary valuable copy from a data medium. Presently, copying is made either at a forensic institution if a body conducting proceedings has applied for an information technology expert analysis to be carried out, or by an investigative body which inspects the data medium seized and needs no specific knowledge or help from an expert. A copy of the data medium is made in the Estonian Forensic Science Institute by an accredited method. However, the police do not have an accredited method for making copies. This means that copies made by an investigative body are usually made in accordance with the discretional power of a particular official, depending on what software and hardware are owned by the official. A body conducting proceedings may appoint an analysis by a digital evidence professional where specific technical knowledge is necessary. Should a body conducting proceedings want a copy of a data medium seized during the search to be made by an accredited method – that is with the intention of ensuring the reliability of the evidence obtained from the data medium is reliable and to the conclusions made therefrom, it cannot ask a forensic institution to make a copy. The making of a copy of a data medium is not an issue for an expert analysis, or to be answered by an expert. The body conducting proceedings make a copy, and, for example, a search for documents from the data medium is executed as an inspection (which does not require any specific expertise, either). It is obvious that the current law does not stipulate precisely enough the procedural needs in this regard. For example, the Slovenian legislature has considered it necessary to regulate an order and conditions for making a copy of a data medium.[30] Taking into account the fact that all subsequent actions aiming at searching for evidentiary information from a data medium are performed by an investigative body with a copy, it is difficult to overestimate the verifiability of this act – the making of a copy.

The opinion of an expert (executed as an expert analyses) or the testimony of an expert explaining an expert analysis together with an inspection report and the appendices are commonly regarded as proofs in the Estonian procedural practice. A copy of the data medium is not attached to these documents, nor is a copy provided to defence counsel as attached to the criminal file. This failure threatens the principle of equality of arms for the parties to legal proceedings.

The audit analysis points out that if a data medium and digital evidence had their own place in a row of strict evidence, there would not be a problem as to how to treat a data medium. The hardware, such as a hard disk, USB stick or smartphone is an item of physical evidence. It has to be established in Estonia whether the physical evidence is conceptually different from the recording obtained from physical evidence. The recording might be considered a document when printed out, as in England & Wales.[31] Other issues that arise include what and how the Prosecutor's Office should submit relevant digital evidence in legal proceedings. Defence counsel must

[29] See Editorial, *Digital Evidence and Electronic Signature Law Review*, 7 (2010), pp 5 – 6 and Editorial, *Digital Evidence and Electronic Signature Law Review*, 9 (2012), pp 5 – 6.

[30] L. Selinšek. 'Electronic evidence in the Slovene Criminal Procedure Act', *Digital Evidence and Electronic Signature Law Review*, 7 (2010), pp 77 – 86.

[31] Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), 10.42-10.51; 10.51.

have the evidence to prepare a defence, and the court must have a copy for the proceeding as evidence. The admissibility of digital evidence must also be considered, as with the authenticity of the evidence.

In conclusion

It has been decided in Estonia that by the year 2020, a criminal file may be digital. Following on from this decision, it is necessary to decide how to incorporate into the law a regulation concerning digital evidence with the aim of seizing as much as possible evidence in its initial digital form, and ensuring the evidence is seized in the place where it is physically located. Taking into account the peculiarities of digital evidence, it is obvious that both legal and technological details require provisions conforming to the requirements of 21st century of establishing fairness and truth in legal proceedings. A balance must be found and maintained between the protection of the fundamental rights of persons and procedural capabilities.

If is a desirable aim that as and when a situation arises, a police officer can start compiling a criminal file in real-time, right at the scene in the street using his or her smartphone (initial evidence, attaching video recordings), then a procedural regulation must ensure safeguards for the parties to criminal proceedings. To investigate an overwhelming majority of criminal offences, digital evidence must be taken both on a national and a cross-border level – that is the peculiar characteristic of digital evidence. The state has a positive duty to protect the rights of its citizens through the penal law, and the effective application of legal protection measures. This means the taking of evidence is also important, which has been a recent object of work for the Ministry of Justice of the Republic of Estonia in cooperation with scientists and practitioners.

Eneli Laurits is a counsellor in the Ministry of Justice in Estonia. Between 2006 and 2015, she worked as a prosecutor, directing pre-trial criminal procedure and represented public prosecution in court dealing with crimes committed against children over the internet and other crimes committed over the internet.

eneli.laurits@just.ee

eneli.laurits@prokuratuur.ee