Preparatory Colloquium
24 – 27 September 2013, Antalya (Turkey)
Section III: Information Society and Penal Law

CROATIA*

Elizabeta IVIČEVIĆ KARAS*

(A) Introduction

Following developments in the field of cyber technology, the new Croatian Criminal Code,[1] which was enacted in October 2011 and came into force on 1 January 2013, incriminates various forms of cybercrime and other criminal offences committed through computer systems. The expanded use of modern technology in criminal activities challenges national legislations to provide efficient criminal prosecution of perpetrators on the one hand, and also to efficiently protect the fundamental human rights of individuals affected by various forms of intrusive procedural measures, on the other hand.

The Croatian Criminal Procedure Act (CPA),[2] which was enacted in December 2008 and partly came into force on 1 July 2009, [3] in comparison with the previous Criminal Procedure Act of 1997 (CPA/1997), which ceased to be in force on 31 August 2011,[4] contains more detailed provisions regarding obtaining ICT-related evidence and it generally widens the use of ICT technology within the criminal procedure.

(B) General Questions

(1) The CPA of 2008 introduced for the first time in the legislation of Croatian criminal procedure the definition of electronic (digital) evidence and the definition of electronic documents which may also be used as evidence in criminal proceedings. The legislator obviously held that the use of classical evidentiary instruments, such as the interrogation of the defendant, the examination of witnesses or expert witness testimony, as well as classical documentary evidence or classical technical recording, was not in line with social developments and with the use of modern technology in criminal activities. In the modern world of ICT, evidence for the needs of the criminal procedure sometimes has to be gathered in a "virtual, electronic world".[5]

According to Article 202 § 32 CPA, "electronic (digital) evidence means data that was collected as evidence in an electronic (digital) form" pursuant to the Criminal Procedure Act. Electronic documents *(elektroničke isprave)*, defined as "briefs which are to be composed in writing and signed according to this Act, may be submitted in the form of an electronic document when they are made, sent, received and stored by the application of available information technologies and provide for establishing a unique marking by which the person who composed the electronic document is identified" (Art. 79 § 1 CPA).

There is only one specific legal provision on electronic (digital) evidence (Art. 331 CPA) which concerns the manner it is obtained. This provision actually refers to other provisions of the Criminal Procedure Act regulating the search of a movable, as well as the temporary seizure of objects (see *infra* D (2)). Although "electronic (digital) evidence" within the Criminal Procedure Act is regulated among other evidentiary actions, electronic evidence in its nature is not actually an evidentiary action, or a type of evidence – it is actually a medium on which the evidence is stored. It is the information that is preserved in an electronic (digital) form that constitutes electronic (digital) evidence. Once it is reproduced, it may have the form of an audio or video recording, a photograph, a written document, etc.

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* Elizabeta Ivičević Karas, Assistant Professor of Criminal Procedural Law, Faculty of Law, University of Zagreb, Croatia.

1 Criminal Code of the Republic of Croatia, Official Gazette 125/2011, 144/2012.

2 Criminal Procedure Act of 15 December 2008, Official Gazette 152/2008, 76/2009, 80/2011, 121/2011, 91/12, 143/2012.

3 Criminal Procedure Act of 15 December 2008 came into force on 1 July 2009 in cases for criminal offences referred to in Article 21 of the Act on Anti-corruption and Organised Crime Prevention Office (Official Gazette 82/2001, 12/2002, 33/2005, 48/2005). For the rest of criminal offences, it came into force on 1 September 2011.

4 Criminal Procedure Act of 3 October 1997, Official Gazette 110/1997, 27/1998, 58/1999, 112/1999, 58/2002, 143/2002, 115/2006.

5 Burić, Z., Prikaz konferencije: Uporaba novih tehnologija u kaznenom postupku – Elektronički dokazi: valjanost i dopustivost elektroničkih dokaza u kaznenom postupku, Barcelona, 26.-27. svibnja 2011., Hrvatski ljetopis za kazneno pravo i praksu, 1/2011, p. 303.

Although the Criminal Procedure Act of 1997 contained provisions on the search of a computer (Art. 211.b CPA/1997), the new Criminal Procedure Act significantly amended and gave greater precision to the previous provisions. This was necessary not only to comply with international obligations, especially the Convention on Cybercrime of 2001,[6] and Recommendation R(95) of the Committee of Ministers of the Council of Europe,[7] but also to respond to practical needs and to clarify certain questions that arose in the jurisprudence of Croatian courts. For example, earlier practice of the Supreme Court of the Republic of Croatia *(Vrhovni sud Republike Hrvatske)* considered that text messages, stored in the memory of a seized mobile telephone, were unlawful evidence if the messages were not obtained through the measure of surveillance and interception of telephone conversations or means of remote communication, in other words through the temporary restriction of the constitutional rights and freedoms that could only be ordered by the investigation judge under specific and strict conditions.[8] However, the more recent jurisprudence of the Supreme Court of the Republic of Croatia considers the search of a mobile phone as the search of a movable, or the search of the contents of records that have remained in the memory of the mobile phone, and not a real-time interception.[9] So there was obviously a need to regulate more precisely at a legislative level the substantive and formal conditions for different measures and evidentiary actions which concern the use of ICT and which affect the fundamental human rights of affected individuals.

(2) The Ministry of Justice *(Ministarstvo pravosuđa)* is a central body of state administration which is in charge of the implementation of ICT within the criminal justice system. Within the General Secretariat of the Ministry of Justice, there is an IT Sector which is responsible for the implementation of ICT - for the development and maintenance of the information system, as well as for providing IT support.[10] More precisely, the IT Sector: a) takes necessary actions for the implementation of ICT within the courts and state attorney offices; b) deals with planning, construction and maintenance of the information infrastructure; c) reconstructs the information system according to legislative changes and the needs of its users; d) deals with information security, and leads and coordinates projects which include an IT component; e) controls the execution of contracts; f) provides direct assistance to users, and coordinates external assistance; g) organises and coordinates training in IT.[11]

Within the Ministry of the Interior, there is a Directorate for Development, Equipment and Support, within which there is a Sector for Information and Telecommunication Technology. Within this Sector, there is an IT Service *(Služba za informatiku),* which is in charge of the development, construction and maintenance of the information system, as well as of information security of the Ministry of the Interior.[12]

Within the Criminal Police Directorate *(Uprava kriminalističke policije)*, there is a National Police Office for the Suppression of Corruption and Organised Crime *(Policijski nacionalni ured za suzbijanje korupcije i organiziranog kriminaliteta (PNUSKOK))*, which includes the Service for Economic Crime and Corruption *(Služba gospodarskog kriminaliteta i korupcije)*. Within this Service, there is a special "Unit for high-technology crime" *(Odjel za visokotehnološki kriminalitet).* This unit carries out the police investigation of criminal offences committed against or through computer systems or networks.[13] It is also in charge of forensic analysis and surveillance of the Internet. This section cooperates with other units within the Ministry of the Interior, providing them with assistance in the police investigation of forms of crime other than economic crime or corruption, when there is a need for expert knowledge in ICT. For example, police officers from this section carry out, upon a court warrant, searches of computers. Furthermore, police officers may also, as expert assistants, participate in the search of a computer and devices connected with the computer, or other devices for the collecting, saving and transfer of data.

(3) In the Republic of Croatia, there are private (commercial) companies that offer ICT-related services to the criminal justice system. For example, INsig2 is a private company which provides services in the field of computer forensics. It offers forensic tools, such as those with various possibilities in the search of evidence, in analysing, presenting and connecting evidence from different sources, in the acquisition of data, etc. The company also organises training for police investigators, court experts and attorneys-at-law in the field of the most recent forensic tools and provides services to the State Attorney's Office, the Ministry of the Interior, the Ministry of Defence, the Ministry of Justice, etc.[14] Another example is the private company

---

[6] Convention on Cybercrime Ratification Act, Official Gazette - International Agreements, 9/2002.

[7] Recommendation of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology, adopted by the Committee of Ministers 11 September 1995.

[8] Supreme Court of the Republic of Croatia, I Kž-75/02-3 of 13 February 2002, I Kž-584/03-3 of 3 March 2005.

[9] Supreme Court of the Republic of Croatia, I Kž 686/06-3 of 8 August 2006; I Kž 901/07-4 of 13 December 2007; I Kž 707/07-3 of 10 April 2008. Ivičević Karas, E., Radnje i mjere procesne prisile radi pribavljanja predmeta za potrebe kaznenog postupka, Hrvatski ljetopis za kazneno pravo i praksu, 2/2008, p. 952.

[10] Article 5 of the Decree on the internal organisation of the Ministry of Justice (*Uredba o unutarnjem ustrojstvu Ministarstva pravosuđa)* of 23 February 2012, Official Gazette 28/2012.

[11] Article 30 of the Decree on the internal organisation of the Ministry of Justice.

[12] http://www.mup.hr/UserDocsImages/minstarstvo/USTROJ_MUP_RH/Sluzba_za_informatiku.pdf

[13] Official website of the Criminal Police, Ministry of the Interior, http://www.policija.hr/159.aspx

[14] http://www.insig2.hr

DataSector d.o.o. which specialises in the field of data recovery.[15] It also provides forensic analysis of computers and mobile phones, and takes part in investigations carried out by the Ministry of the Interior, through cooperation with forensics experts in IT.[16] A further example is Borea d.o.o., a private company which offers services in the field of IT security. It provides computer forensics services in detecting and solving security incidents.[17] The activity of the company includes forensic analysis of computers and the net, ranging from making accurate copies and reviewing the data, right through to analysing data on net resources.[18] Therefore, it is possible to conclude that a private sector is involved in providing ICT-related services to the criminal justice system in the Republic of Croatia.

(C) Information and Intelligence: building information positions for law enforcement

(1) Within the Ministry of Interior, the Police Directorate *(Ravnateljstvo policije)* adopted and implemented the concept of "intelligence-led-policing" (ILP) in order to support investigation of serious crime and strategic planning. Therefore, police authorities have competence to build information positions. The ICT-related techniques used for building information positions for police authorities while conducting inquiries into criminal offences include accessing various public and private databases and comparing those data with police data records, registers and automatic data-processing bases.

Besides police forces, the intelligence services also have access to various public and private databases in order to gather information within their competences. There are only limited possibilities to use coercive measures involving ICT-related techniques for building information positions for intelligence services, and only under strict conditions (see below).

(2) In order to establish the identity of the suspect, police authorities may take non-intimate samples for molecular genetic analysis from the suspect of a criminal offence for which a punishment of imprisonment is prescribed, even without his consent (Art. 211 § 1 and 3 CPA). These data on identity may be entered into the data collections and databases with automatic data processing. The structure and the manner of keeping these databases are regulated by Regulations adopted by the Minister of the Interior.[19] According to Article 2 of the Regulations, the collection of DNA profiles is established and managed in the IT system of the Ministry of the Interior. This collection contains, among other data, the DNA profile and complete or partial DNA profiles of traces collected from the crime scene.

Taking samples of biological materials from the place where the criminal offence was committed may be ordered by the authority (including police authorities) conducting the search, the temporary seizure of objects, an investigation on the scene of a criminal offence or other evidentiary action prior to the commencement of the proceedings (Art. 327 § 4 CPA). However, only the authority conducting the criminal proceedings, a state attorney or the court may order molecular genetic analysis if a probability exists that data important for proving the criminal offence would be obtained by such an analysis (Art. 327 § 1 CPA). For this purpose, the authority conducting the proceedings may, prior to and pending criminal proceedings for a criminal offence prosecuted ex officio, order the taking of samples of biological material from the place where the criminal offence was committed and from another place where there are traces of a criminal offence, from the defendant, from the victim and from another person (provided that it is not a biological sample of that person), unless otherwise prescribed by the Criminal Procedure Act (Art. 327 § 2 CPA).

Regarding financial data, a state attorney may ask for data from banks only for the need of a certain criminal investigation. If the bank denies access to data considered to be a bank secret, the state attorney may request the court to issue a court order (Art. 265 §1 CPA). The court also stipulates the term within which the bank must hand over the data to the state attorney. This means that financial data considered to be a bank secret are protected in a way that banks are actually not obliged to reveal them, unless upon a court order. At the request of a state attorney, a court may also order the bank to deliver data related to a person's account when it is probable that that person "receives, holds or disposes in any other way of income arising from a criminal offence on his bank account and this income is important for the investigation of that criminal offence or that it may be seized by force pursuant to law" (Art. 265 § 2 CPA). These measures are regulated by the Criminal Procedure Act within the formal evidentiary action of the temporary seizure of objects.

(3) Verification of personal data *(sravnjivanje osobnih podataka)* is another possibility for law enforcement agencies to use ICT-related techniques for building information positions. "The police authorities may compare personal data of citizens kept in a database and other registers with police data records, registers and automatic data processing bases, provided that there are grounds for suspicion that a criminal offence prosecuted ex officio has been committed" (Art 340 § 1 CPA). Verification of personal data implies collating personal data which are stored in various collections and registers (for example, records regarding the verification of identity, transit over the border, registered revenue, etc.) with police registers

[15] http://www.datasector.hr/o-nama
[16] http://www.datasector.hr/forenzika
[17] http://www.borea.hr/usluge/racunalna-forenzika-8-11
[18] http://www.borea.hr/usluge/forenzicka-analiza-racunala-i-mreze-8-29
[19] Regulations on the organisation and the manner of managing collections with automatic processing of data on establishing the identity of the suspect *(Pravilnik o ustrojstvu i načinu vođenja zbirki s automatskom obradom podataka o utvrđivanju istovjetnosti osumnjičenika),* Official Gazette 157/2009.

and collections containing an electronic database. The gathered data may be used to create a "profile" of a potential perpetrator, as well as indicators of a suspect.[20] However, the information collected through verification of personal data serves primarily for the identification of a perpetrator and therefore "must be erased as soon as it ceases to be necessary for successfully conducting criminal proceedings, at the latest twelve months from the day when it was stored". Prolongation is possible only exceptionally "if it is probable that in such a manner pursuit of a certain person or object may be successfully completed", and it must be ordered by the judge of investigation (Art. 340 § 1 CPA).

According to Article 25 of the Act on the Security Intelligence System of the Republic of Croatia (ASIS),[21] intelligence forces may gather information, within their competences, through communication with citizens and by requesting official data from state bodies and legal persons, including the consultation of registers, data collections and official documentation. The consultation of data collections or documentation may be conducted either through direct insight, or through permanent access to a computer data collection through the use of appropriate interfaces (Art. 31 ASIS).

(4) According to Article 68 of the Police Services and Competences Act (PSCA),[22] a police officer may claim from telecom providers the verification of identity, duration and frequency of contacting certain telecommunication addresses, in order to: a) prevent danger, b) prevent violence and c) prevent and discover a criminal offence which is prosecuted ex officio. This verification may include the determination of the locations of persons establishing the telecommunication contacts, as well as the identification marks of the device, but it does not include the interception of telecommunication content data. It should be stressed that the police may not gather the data directly through the application of specific computer programmes, but only indirectly through telecom providers.[23] Verification may be carried out only upon written authorisation issued by the Head of the Criminal Police, or by another person that he or she authorises. There is no judicial control provided on this police action.

Besides police authorities, intelligence forces have the authority to gather information, but also to use coercive powers in their preventive tasks, primarily in order to protect national security, but also to prevent crimes such as terrorism, other forms of organised violence, as well as organised and economic crime.[24] According to Article 33 of the Act on the Security Intelligence System of the Republic of Croatia, the Security Intelligence Agency (SOA) (and the Military Security Intelligence Agency (VSOA), but only regarding Ministry of Defence personnel), may use measures for the secret collection of data if it is necessary for the protection of state security and when the information cannot be gathered in any other way or if its gathering would involve great difficulties. Secret collection of data includes measures such as secret surveillance of telecommunication, secret electronic surveillance of premises and objects, secret surveillance by recording persons in open areas and public places, and secret surveillance and video and audio technical recording of persons and their conversations in public places. The secret surveillance of telecommunication includes the contents of communication, data on telecommunication traffic, the location of the user, and/or international telecommunication links.

Secret surveillance may be proposed by the Director of the Intelligence Agency and ordered by a written warrant with a statement of reasons issued by a Supreme Court judge. Only exceptionally, if there is a danger of delay, may the Director of the Intelligence Agency himself order secret surveillance, but upon his report, the competent Supreme Court judge must issue a warrant of approval within 24 hours from the beginning of the application of the measure. If a warrant is not issued, the measure has to be interrupted and all the produced documents and materials have to be destroyed (Art. 36 § 2 ASIS). Secret surveillance may last up to four months, and can be prolonged for another three months.[25] It is important to stress that, having practically the same legal value as the official notes of the police, intelligence information is not admissible as evidence in the criminal procedure. However, intelligence information may be used as "preliminary information for opening criminal investigation".[26]

(5, 6) According to Article 68 of the Police Services and Competences Act, telecommunication providers have to provide, on the request of the police, data on the verification of the identity, duration and frequency of contacting certain telecommunication addresses, on the locations of persons establishing the telecommunication contacts, as well as the identification marks of the device. According to Article 19 of the Act on the Security Intelligence System of the Republic of Croatia, all legal and natural persons who operate telecommunication networks and provide public telecommunication services are obligated not only to provide direct and permanent access to objects and technical equipment for the secret

[20] Krapac, D., Kazneno procesno pravo, Prva knjiga: Institucije, Narodne novine, Zagreb, 2012., p. 348-349.
[21] Act on the Security Intelligence System of the Republic of Croatia *(Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske),* Official Gazette 79/2006, 105/06.
[22] Police Services and Competences Act *(Zakon o policijskim poslovima i ovlastima),* Official Gazette 76/2009.
[23] See Pajčić, M., Korištenje forenzičnim računalnim programima za prikupljanje dokaza u kaznenom postupku, Hrvatski ljetopis za kazneno pravo i praksu, 1/2009, p. 307.
[24] See Đurđević, Z., Preparatory Colloquium of the XVIII International Congress of Penal Law, Section III, Pula (Croatia), 6-9 November 2008, p. 118.
[25] *Ibid.*, p. 118-119.
[26] *Ibid.*, p. 117-118.

surveillance of telecommunication by the Operational Technical Centre for Surveillance of Telecommunications (OTC),[27] but also to keep data on telecommunication traffic in the previous year, and to deliver data on all communication devices which appeared at a certain geographic, physical or logical location, regardless of the telecommunication activities, in the period of the previous 48 hours.

(7) The principal rule regarding police authorities building information positions is, on one hand, that there is no judicial control. Information gathered through building information positions serve as evidence in a "cognitive sense" which should direct the criminal investigation and the taking of formal evidentiary actions. On the other hand, building information positions by intelligence services through the use of ICT is subject to judicial control, as described above, since covert coercive measures may only be taken following a warrant issued by a Supreme Court judge. However, measures such as gathering information through communication with citizens and by requesting official data from state bodies and legal persons, including the consultation of registers, data collections and official documentation, are not subject to judicial control.

(D) ICT in the criminal investigation

(1) For the needs of the pre-trial procedure, there is the possibility of interception in real time of both traffic data and content data. These measures are carried out within "special evidentiary actions" which are conducted covertly regarding the targeted person, and which "temporarily restrict certain constitutional rights of citizens" (Art. 332 § 1 CPA). They consist of "surveillance and technical recording of telephone conversations and other means of remote communication" (Art. 332 § 1 (1) CPA).or of "the interception, gathering and recording of computer data" (Art. 332 § 1 (2) CPA). There are no specific provisions on special evidentiary action of "the interception, gathering and recording of computer data" which would allow the possibility to obtain electronic evidence through remote forensic computer programs.[28]

The substantive preconditions for applying special evidentiary actions are that "the investigation cannot be carried out in any other way or would be accompanied by disproportionate difficulties" and that "there are grounds for suspicion" that the person "committed or has taken part together with other persons in committing" an offence which is listed in a catalogue of offences.[29] The formal precondition is a written warrant with a statement of reasons, which may be issued by the judge of investigation upon the written request, accompanied by a statement of reasons, of a state attorney. Only exceptionally, "when circumstances require that the actions are to commence immediately", may the state attorney issue a warrant "prior to the commencement of the investigation for a term of twenty-four hours", but he "must deliver the warrant with a note on the time of issue and a statement of reasons to the judge of investigation within the term of eight hours from the issue" (Art. 332 § 2 CPA). The judge of investigation decides on the legality of the warrant. However, these provisions, although still existing in the legislative text, have actually been vacated by the Decision of the Constitutional Court of the Republic of Croatia,[30] which held that the contents of the provision of Article 332 § 2 of the Criminal Procedure Act is undefined and unclear, and that its effects are unclear and unpredictable.[31] So this legislative provision will have to be amended until 31 December 2013 at the latest, in order to comply with the Constitution.

Special evidentiary actions, including the surveillance and technical recording of telephone conversations and other means of remote communication, as well as the interception, gathering and recording of computer data, may last up to six months at the most. On the motion of a state attorney, the judge of investigation may, "on account of important reasons", prolong the duration of such measures for a term of another six months, and then again for a further term of six months, in "specially complex cases" (Art. 335 § 3 CPA). These provisions have also been vacated by a Decision of the Constitutional Court of the Republic of Croatia,[32] which considered that the legal notions, such as "on account of important reasons" and "especially complex cases" were undefined.[33] The Constitutional Court also considered that the prolongation of deadlines may only be

[27] The Operational Technical Centre for Surveillance of Telecommunications (OTC) is provided for in Article 18 of the Act on the Security Intelligence System of the Republic of Croatia. The OTC activates and manages the measures of secret surveillance of telecommunication services, whether they are regulated by the Criminal Procedure Act or the Act on the Security Intelligence System of the Republic of Croatia. It also coordinates and supervises legal and natural persons who operate public telecommunication networks and provide public telecommunication services and the bodies in charge of measures of secret surveillance.

[28] See Pajčić, M., *supra* note 23, p. 310-313.

[29] The catalogue of offences is listed in Article 334 of the Criminal Procedure Act, which refers to both Criminal Code of 1997 (Official Gazette 110/1997, 27/1998, 50/2000, 129/2000, 51/2001, 111/2003, 190/2003, 105/2004, 84/2005, 71/2006, 110/2007, 152/2008, 57/2011, 77/2011) and the new Criminal Code of 2011. The catalogue includes, besides other severe criminal offences, cyber crimes and other criminal offences committed through computer systems such as child pornography on a computer system or network (Art. 197a CP/1997), infringement of secrecy, integrity and accessibility of computer data, programs and systems (Art. 223 CP/1997), computer forgery (Art. 223a CP/1997), computer fraud (Art. 224a CP/1997). It also includes all criminal offences against computer systems, programs and data (Chapter XXV CP/2011) punishable by imprisonment for a term of five years or more.

[30] Constitutional Court of the Republic of Croatia *(Ustavni sud Republike Hrvatske),* U-I-448/2009, U-I-602/2009, U-I-1710/2009, U-I-18153/2009, U-I-5813/2010, U-I-2871/2011 of 19 July 2012, Official Gazette 91/2012, point 162.

[31] See Krapac, D., *supra* note 20, p. 336.

[32] Constitutional Court of the Republic of Croatia, *supra* note 30, point 170.

[33] See Krapac, D., *supra* note 20, p. 337.

exceptional, and only if the evidence could not be gathered in a manner which would less infringe the constitutional rights of citizens.

According to the Criminal Procedure Act, special evidentiary actions of surveillance and technical recording of telephone conversations and other means of remote communication and special evidentiary actions of interception, gathering and recording of computer data are all executed by police authorities, who draw up daily reports on the process of execution and the documentation of the technical transcript, which they deliver to the state attorney upon his request (Art. 337 § 1 CPA). "Upon the termination of the action, the police authorities draw up a special report for the state attorney's office and the judge of investigation stating as follows: 1) the time of the commencement and time of the termination of the action; 2) the number and identity of persons covered by the action" (Art. 337 § 2 CPA). Although still prescribed in the Criminal Procedure Act, these provisions have been declared unconstitutional and have been vacated by a Decision of the Constitutional Court of the Republic of Croatia, which considered that there were deficiencies in the mechanism of the state attorney's and the court's control over the application of these actions, since there was no obligation for the police to deliver daily reports and documentation of the technical transcript to the judge of investigation and the state attorney. Therefore, the judge of investigation does not have access to information relevant to assess how well grounded the application of evidentiary action in the whole procedure is.[34] Therefore, a legislative amendment is expected, which should provide mechanisms for efficient state attorney and judicial control of the execution of special evidentiary action.

(2) The Criminal Procedure Act provides that, unless otherwise prescribed by the Criminal Procedure Act, electronic evidence shall be obtained by applying the general provisions regulating the search of a movable, including a computer and devices connected with the computer, other devices for the collecting, saving and transfer of data, telephone, computer and other communications, as well as data carriers (Art. 257 CPA). Upon the request of the authority carrying out the search, which can be a state attorney, an investigator or police forces, the person using the computer or having access to the computer or other device or data carrier, as well as the telecommunications service provider, must enable access to the computer, device or data carrier and give necessary information for its undisturbed use and for the fulfilment of the objectives of the search. These persons also must immediately undertake measures to prevent the destruction or change of data. Such measures can also be undertaken by an expert assistant, but only upon the order of the authority carrying out the search. There is no legislative provision that an expert assistant could be ordered to take measures necessary to access the data contained in the computer and other devices, for example in cases where the computer must first be repaired in order to enable it to be an object of the search.[35]

In the case where a private person, with the exception of the defendant, fails to comply with his or her obligations, he or she may be punished with fine not exceeding HRK 50,000.00. If he or she still does not comply, he or she may be punished by imprisonment until the request is executed, but for no longer than one month (Art. 257 § 3 and Art. 259 § 1 CPA).

Besides provisions on the search, provisions regulating rules on the temporary seizure of objects also apply to obtaining electronic evidence (Art. 261 and Art. 263 CPA): they apply to data saved on a computer and devices connected thereto, as well as on devices used for the collecting and transferring of data, data carriers and subscription information which is in the possession of the service provider, except in the case where temporary seizure is explicitly prohibited by the Criminal Procedure Act. According to Article 263 of the Criminal Procedure Act, these data must be handed over to the state attorney upon his written request in an integral, original, legible and understandable format, in a term stipulated by the state attorney, otherwise sanctions are imposed (see above). The collected data shall be recorded in real time by the authority carrying out the action, respecting the regulations regarding the obligation to observe confidentiality in the recording, protecting and storing of the data. In accordance with the circumstances, data not related to the criminal offence for which the proceedings are conducted, and are required by the person against which the measure is applied, may be recorded on an appropriate device and be returned to this person even prior to the conclusion of the proceedings.

Upon a motion of the state attorney, the judge of investigation may decide on the protection and safekeeping of all data collected from a computer and other devices, for as long as necessary and for six months at the most. After this term, the data shall be returned, unless they have been used in the commission of a specific "cybercrime" or other criminal offences committed through computer systems, or if they are used as evidence of a criminal offence for which proceedings are being conducted.

(3) According to Article 335 § 2 of the Criminal Procedure Act, "the technical operative centre for the supervision of telecommunications that carries out technical coordination with the provider of telecommunication services in the Republic of Croatia as well as providers of telecommunication services shall be bound to provide the necessary technical assistance to the police authorities". In the case of non compliance and proceeding contrary to this obligation, the judge of investigation shall, upon a motion with a statement of reasons of the state attorney, impose a fine on the provider of telecommunication services in an amount not exceeding HRK 1,000,000.00. A sanction shall also be imposed both on the responsible person in

[34] Constitutional Court of the Republic of Croatia, *supra* note 30, point 171-174.
[35] Ivičević Karas, E., *supra* note 9, p. 952-953,

the technical operative centre for the supervision of telecommunications that carries out technical coordination, and on a provider of telecommunication services in the Republic of Croatia, in an amount not exceeding HRK 50,000.00. If, thereafter, the ruling is not complied with, the responsible person may be punished by imprisonment until the ruling is executed, but for no longer than one month. There is a possibility of appeal against the ruling on the fine and imprisonment, but the appeal does not stay its execution.

In the case of the evidentiary action of a search of a computer, according to Article 257 § 1 of the Criminal Procedure Act, upon the request of the authority carrying out the search of a computer (a state attorney, investigator or the police), not only the person using the computer or having access to the computer but also the telecommunications service provider must enable both access to the computer, device or data carrier, and provide necessary information "for its undisturbed use and for the fulfilment of the search objectives". They must also, upon the order of the authority carrying out the search, "immediately undertake measures for preventing the destruction or change of data" (Art. 257 § 2 CPA). If a service provider fails to comply, it may be punished with a fine not exceeding HRK 50,000.00. Even if after such a fine it does not comply, it may be punished by imprisonment until the request is executed, but for no longer than one month (Art. 257 § 3 CPA).

(4) According to Article 79 § 1 of the Police Services and Competences Act, the police may record public places using audio-video devices in order to prevent criminal offences which are prosecuted ex officio, as well as misdemeanours. According to Article 79 § 2 of the Police Services and Competences Act, on the occasion of a public gathering, if there is a danger to people's life and health or to property, the police are permitted to audio- and video- record and photograph the public gathering. In both of these cases, the police must beforehand and publicly announce the intention to make the recording.[36] If a criminal offence occurs during the recording of a public place using audio-video devices, this recording may be used as evidence in criminal proceedings as a "public recording".

Video surveillance may be applied as a covert, special evidentiary action of "entry into the premises for the purpose of conducting surveillance and technical recording of the premises", and/or the "covert following and technical recording of individuals and objects (Art. 332 §1 (3) and (4) CPA)". The substantive and formal preconditions for applying these measures are the same as those prescribed for the special evidentiary actions of "surveillance and technical recording of telephone conversations and other means of remote communication" or of "the interception, gathering and recording of computer data" (see *supra* D (1)). These measures are covert and coercive towards a person against whom there are grounds for suspicion that he committed or has taken part together with other persons in committing an offence listed in the catalogue of offences. However, these measures may be applied to the means, premises and objects of other persons only with their written consent (Art. 332 § 5).

There is no legislative provision stipulating the obligation of natural or legal persons to cooperate with law enforcement agencies in applying video surveillance.

(5) During the pre-trial proceedings, evidentiary actions, including the interrogation of suspects and witnesses, are conducted by a state attorney, or an investigator upon his order (Art. 213 § 1 CPA). The first interrogation of the defendant, conducted by the state attorney or the investigator, must be recorded by an audio-video recording device, which is operated by an expert person (Art. 275 § 2 CPA). The audio-video recording of the first interrogation of the defendant is always obligatory, otherwise the protocol on the interrogation of the defendant may not be used as evidence in proceedings (Art. 281 CPA). Further interrogations may be recorded upon a decision of the authority conducting the interrogation, but the recording is not obligatory.

The defendant may be confronted with a witness or another defendant if their statements do not correspond regarding important facts. If the confrontation takes place during investigation, it must be recorded by an audio-video recording device. If the confrontation has not been recorded, the protocol on confrontation may not be used as evidence (Art. 278 § 1 and 4 CPA).

The interrogation of witnesses, as a rule, is not recorded by an audio-video device. However, if the interrogation of the witness is undertaken through an interpreter or if the witness is deaf or mute, the interrogation carried out through an interpreter may be recorded by an audio-video recording device. In this case, the recording must be enclosed with the protocol (Art. 290 CPA). The interrogation of a child younger than 14 as a witness is carried out by the judge of investigation and is always recorded by an audio-video recording device (Art. 292 § 1 CPA). The interrogation of a child aged over 14 but less than 18 years may also be recorded, but this is not obligatory (Art. 292 § 2 CPA).

Witnesses who cannot obey the summons due to their old age, state of health, serious physical disabilities or mental state may be interrogated in their dwellings or other premises where they are situated, through audio-video devices which are operated by an expert assistant. The interrogation may be recorded (Art. 292 § 3 CPA). The same rule applies to the interrogation of a victim of a criminal offence against sexual freedom and sexual morality, or if a criminal offence is committed in the family, but only upon the victim's request (Art. 292 § 4 CPA). The judge of investigation may order that the

[36] In order to supervise the state border, the police may also make a recording of the area of the state border and border crossings.

interrogation of a protected witness be recorded by an audio-video or an audio recording device, taking special care of the protection of the witness (Art. 297 § 2 CPA).

A witness may be confronted with another witness or by the defendant if their statements do not correspond regarding important facts. The confrontation must be recorded by an audio-video recording device and the recording is enclosed with the protocol. If the confrontation has not been recorded, the protocol may not be used as evidence in criminal proceedings (Art. 289 §§ 4 and 5 CPA).

Finally, when the Criminal Procedure Act so prescribes, "a trial, an evidentiary action or any other action may be recorded by audio-video or audio recording devices". However, the authority conducting the evidentiary action may always decide that evidentiary action be recorded by audio or audio-video recording devices, but must inform the participating persons that the action is being recorded by a particular technical device and that the recording may be used as evidence in the proceedings (Art. 87 §§ 2 and 3 CPA). The recording must contain information on the name of the authority before which the procedural action is being undertaken, the place where it is undertaken, the day and hour when it is commenced and completed, the names and surnames of the persons present, as well as their role in the proceedings, and the identification of the criminal case in which the action is undertaken, as well as information necessary to determine the identity of the person whose statement is being recorded and information regarding the procedural role of that person (Art. 87 § 4 CPA). Upon the request of the interrogated person, the recording shall be reproduced immediately and corrections or explanations made by this person shall be recorded.

In the case of recording the evidentiary action, the protocol must, along with other information, contain information that a technical recording was made, who did the recording, which device was used in making the recording, that the interrogated person was previously informed that the recording would take place, a short summary of the given declarations and statements, whether the recording was reproduced and where the recording is kept if it is not attached to the case files (Art. 87 § 5 CPA).

(E) ICT and evidence

(1) Regarding obtaining electronic evidence, the Criminal Procedure Act provides that, unless otherwise prescribed by the CPA, electronic evidence shall be obtained by applying the general provisions regulating the search of a movable, including a computer and devices connected with the computer, other devices for the collecting, saving and transfer of data, a telephone, computer and other communications, as well as data carriers (Art. 257 CPA), as described above. The provisions containing rules on the temporary seizure of objects also apply to obtaining electronic evidence (Art. 261 and Art. 263 CPA) (see *supra* D (1)).

(2) According to Article 430 of the Criminal Procedure Act, the presentation of electronic evidence shall be performed in the manner regulated by provisions on documentary evidence (Art. 329 CPA), recording evidence (Art. 330 CPA) and electronic (digital) evidence (Art. 331 CPA). Regarding recording evidence, the Criminal Procedure Act explicitly prescribes that the procedures shall be the same as those regarding other objects that are to be used as evidence, "paying attention not to damage or destroy the recording and to keep its content in an unchanged condition". It is also added that if necessary a copy should be made (Art. 330 § 2 CPA).

The competent minister is obligated by the Criminal Procedure Act (Art. 572 CPA) to introduce more detailed regulations on technical conditions, the methods for recording and the protection of the recording from deletion or damage. The Minister of Justice has therefore brought Regulations on the recording of evidentiary actions or other actions in pre-trial and criminal proceedings.[37] The Regulations contain provisions on the technical conditions and the methods of audio-video recording of the first and later examinations of the defendant and evidentiary or other actions, protection of the recording from deletion and damage, and the methods of keeping the recording. Once the recording of evidentiary action is completed, the copy is sealed and it forms an integral part of the protocol on evidentiary action. The recording of the first interrogation of the defendant is sealed and handed over to the judge of investigation. One copy is for the defendant and the other for the state attorney.

As a rule, the contents of the recording are determined through its reproduction and always by an expert person (Art. 330 §§ 3 and 4 CPA).

(3) In Croatian law, there are no rules on admissibility of evidence that would be specific for ICT-related information. The general rules on unlawful evidence, proclaimed in Article 10 of the Criminal Procedure Act, apply to electronic evidence or to any other ICT-related information and evidence.

(4) In Croatian criminal procedural law, there are no specific rules on discovery and disclosure for ICT-related evidence.

(5) In Croatian criminal procedural law, there are no special rules for evaluating ICT-related evidence. The general rule applies, according to which the right of the court and state authorities participating in criminal proceedings to assess the

[37] Regulations on recording of evidentiary actions or other actions in pre-trial and criminal proceedings *(Pravilnik o snimanju dokazne ili druge radnje u prethodnom i kaznenom postupku),* Official Gazette 92/2009, 15/2010, 120/2011.

existence or non-existence of facts must not be bound or restricted by special rules of evidence, although these bodies are obligated to clearly state the reasons for the decisions they make (Art. 9 CPA). So, the court is bound to conscientiously assess each ICT-related piece of evidence "individually and in relation to other evidence" and on the basis of such an assessment the court must "reach a conclusion on whether or not a particular fact has been proved" by the means of electronic evidence (Art. 450 § 2 CPA). The same rule applies regarding the evidentiary value of an electronic document. If an electronic document is composed in accordance with the provisions of the Electronic Signature Act[38] and the Electronic Document Act,[39] it is assessed in the same way as the evidentiary value of any "classical" document.

For example, if the search of a mobile phone is conducted on the basis of a valid court order, the results of that search may be used as evidence. If the defendant claims that the police officer could have maliciously entered data in the memory of the mobile phone, such a claim is considered by the Supreme Court of the Republic of Croatia as a "common hypothesis" which is not supported by the rest of the file; in the circumstances of the specific case, the Supreme Court could not see "what the motivation of the police officers would possibly be".[40]

Anyway, regarding the evaluation of electronic evidence, the bodies conducting criminal proceedings in the earlier stage, and the court during the trial, will often be in such a position that they have to use experts in digital or computer forensics, since these experts will provide the court with information regarding whether the ICT-related evidence was obtained in a technically correct manner. They will also provide information on the credibility of the evidence.[41] On the basis of such information, the court will be able to evaluate the ICT-related evidence.

(F) ICT in the trial stage

(1) According to Article 430 of the Criminal Procedure Act, in the evidentiary proceedings at the trial stage, the presentation of electronic evidence shall be performed in the manner regulated by the provisions on documentary evidence (Art. 329 CPA), recording evidence (Art. 330 CPA) and electronic (digital) evidence (Art. 331 CPA) (see *supra* E (2)).

(2) The Croatian Criminal Procedure Act provides the possibility for the application of distant interrogations. Article 192 § 1 of the Criminal Procedure Act stipulates that "except for cases specified in this Act, the court may, by a written order, order that the evidentiary hearing be conducted by means of a closed technical device for remote connection (audio-video conference)". The Court may pose questions directly to the interrogated person, while the parties "may be present at the audio-video conference and take part in it pursuant to the provisions of Article 292 paragraph 3" (Art. 193 § 1 CPA). An expert person operating the devices must be present at the audio-video conference (Art.193 § 2 CPA). The authority conducting the proceedings makes a protocol on the audio-video conference, indicating the time and place of the action, the persons who were present, the type and state of the technical devices for remote connections and the expert person who operated the device (Art. 194 § 1 CPA).

(3) Digital and virtual techniques can be used for the reconstruction of events. The rules on the application of such techniques are not contained in the Criminal Procedure Act or in legislation in general, but they are contained within the rules of certain professions. For example, in practice, appointed experts often use in their expertise various digital and virtual techniques, such as 3D reconstructions of traffic accidents, killings, etc. The documentation on such expertise constitutes an integral part of the case files, and such documentation is presented before the court at the trial stage.

(4) Audio-video techniques can be used to present evidence at the trial. Moreover, unless otherwise prescribed by the Criminal Procedure Act, the contents of the audio and/or video recording, including digital recording, must be determined through its reproduction (Art. 330 § 3 and Art. 430 CPA) before the court at the trial. When the Criminal Procedure Act stipulates that, besides the recording of certain evidentiary action, the protocol is made with certain data only, the recording must be reproduced and the protocol must be read before the court (Art. 432 § 1 CPA). Moreover, "the panel may always decide that besides reading the protocol at the trial, a recording of the interrogation be reproduced" (Art. 432 § 2 CPA). These rules are in accordance with the principle of direct presentation of evidence before the court.

(5) In Croatian criminal proceedings, there are still only classical criminal "paper" files that cannot be replaced by "electronic ones". However, there have been recent developments in digitalising parts of the file. As described above, evidentiary actions, including the interrogations of defendants and examination of witnesses, either must or can be recorded on a CD or DVD, and the recordings constitute an integral part of the file.

Finally, it should be mentioned that the Court Rules *(Sudski poslovnik)*[42] provide for the establishment of an "eFile" *(eSpis)* which offers a unique information system for administering court cases. Once the technical and organisational conditions are fulfilled, each court will start to use the eFile system upon the decision of the Minister of Justice.

---

[7] *Electronic Signature Act (Zakon o elektroničkom potpisu),* Official Gazette 10/2002, 80/2008.
[39] Electronic Document Act *(Zakon o elektroničkoj ispravi),* Official Gazette 150/2005.
[40] Supreme Court of the Republic of Croatia, III Kr 193/09-11 from 6 May 2010.
[41] Krapac, D., *supra* note 20, p. 503-504.
[42] Article 3 of the Court Rules *(Sudski poslovnik)*, Official Gazette 158/2009, 3/2011, 34/2011, 100/2011, 123/2011, 138/2011, 38/2012, 111/2012.