



Enhancing procedure of using new means of technologies in criminal proceedings

REFORZANDO EL PROCEDIMIENTO PARA EL USO DE NUEVOS MEDIOS TECNOLÓGICOS EN LOS PROCEDIMIENTOS PENALES

Delia Magherescu

State University of Moldova
delia_magherescu@yahoo.com

Recibido: 20 de febrero de 2020 | Aceptado: 11 de mayo de 2020

ABSTRACT

The new era of technology is currently of high interest for the judicial proceedings in criminal matters. Although digital technologies have been increased in the last decades, both legislator and judicial authorities being involved in developing more and more efficient means of forensic investigation in purpose to prevent and combat the criminal phenomena, the criminal organizations are also interested in breaking such legal digital framework and achieving their own scope - a financial one. On the one hand, they are permanently interested in committing serious crimes including those in digital environment, whose consequences are one of the most dangerous crimes for the entire contemporary society. On the other hand, the law enforcement agencies are working in close cooperation with experts in digital field in order to gather information on how to improve the situation itself and investigate the criminal activities by means of digital evidence. In this context, the digitalization is an efficient tool of providing information, data and other instruments the judicial bodies need in achieving their goals in criminal proceedings. The current paper focuses on the techniques and methods that judicial bodies use in the investigation activity of gathering digital evidence that may serve in making decision in criminal cases the judicial bodies are invested with. The paper is structured in five chapters, each of them providing referential elements on the proposed topic. Its structure is designed as follows: Introduction; Aims; Methodology of Research; Achievements and failures through using new technologies; Doctrinal and jurisprudence approach, and Conclusion section, which advances a *de lege ferenda* proposal.

KEYWORDS

Criminal proceedings
Digital technology
Forensic evidence
Judicial bodies
Means of technologies

INTRODUCTION

The new era of technology and its implication in the field of criminal proceedings is so current as it is met in the field of jurisprudence. The decisions pronounced by the courts of law are now more accustomed to solutions stated in such criminal cases also solved through digital evidence and digital technologies. This means that several kinds of crimes are committed in a digital environment, as consequence of the new technologies used frequently by the perpetrators, in particular by the organized criminal groups. Their main purpose is that of achieving huge amount of money in a short period of time and using a low level of investment.

Actually, the digital technologies appear in this contest as efficient skills also preferred by the criminal groups in order for them to commit serious crimes including the organized criminal activities in digital environment. In practice, it is frequently confirmed that the criminals are concerned with digital evidence and, for this reason, they "will attempt to manipulate computer systems to avoid apprehension"¹, on the one hand. In order to avoid any repercussion in criminal investigation activity, digital investigators cannot simply rely on what is written in manuals of good practice in investigation, but additionally they must be accustomed with the specific techniques and case studies which provide "general concepts and methodologies that can be applied to new situations with some thought and research (...)", on the other hand².

All these aspects make the judicial authorities analyse the *de facto* situation and reflect upon a more comprehensive way in the field of judiciary to combat them. For this reason, a kind of "judicial competition" is featured between criminal activities of criminal organized groups and the judicial bodies, who are permanently looking for being one step ahead the criminality in purpose to discover all crimes committed³ and punish the perpetrators in accordance with their guilt⁴.

The introductory section highlights particular feature of the digital means of procedure and evidence as well as the other issues provided by scientific tools being integrated in the digital environment as well.

Usually, using new means of technology in criminal proceedings is frequently associated with digital crimes, but there are still certain offenses, such as those stated earlier, which also are investigated and judged through digital evidence.

Analyzing the procedure from a technical point of view, the legislation does not impose any limitation between serious crimes or petty offenses. As a consequence, all offenses which are committed or lead with digital context can be investigated and judged

1. Casey, E., *Digital evidence and computer crime*. Third Ed., Maryland: Elsevier, 2011, p. 10.

2. *Ibidem*.

3. Dzehtsiarou, K., "European Consensus and the Evolutive Interpretation of the European Convention on Human Rights", *German Law Journal*, 2011, 12(10), pp. 1730-1745. <https://doi.org/10.1017/S2071832200017533>

4. According to Article 6 of the European Convention of Human Rights of 1950, entered into force in 1953, Council of Europe, Cedex, Strasbourg, available online at: https://www.echr.coe.int/Documents/Convention_ENG.pdf

by means of digital evidence. The only one requirement the legislation imposes is that they must be gathered legally and, once administered, they must be pertinent, conclusive and genuine⁵.

AIMS

The activity of research conducted on the topic of enhancing procedure of using new means of technology in criminal proceedings has identified a series of particularities over the several forms of gathering evidence by the judicial bodies and administering them in front of the court of law in cases of serious crimes including those committed in a digital context.

The digital context is currently more comprehensive in this matter and, for this reason, the aims established at the beginning the the research study were outlined in accordance with the entire used methodology of research.

In the procedure of gathering digital evidence and administering them by the judicial bodies, both during the investigation and judgment phases of penal proceedings, the main aims of the current paper are related to the following issues:

- new technologies in digital field provide the investigation bodies with more developed procedures and techniques during the criminal proceedings in order to solve the penal cases;
- legal limitations imposed by the constitutional principles in the area of guaranteeing citizens' fundamental rights and liberties also stated by the European Convention on Human Rights and the EU treaties and other provisions adopted by the EU institutions, which are compulsory by the all Member States;
- new mechanisms of investigation in criminal proceedings developed from new means of digital technologies;
- using new digital evidence in criminal proceedings as well as the special simplified procedure of investigating and judging penal cases in a reasonable time;
- analyzing the judicial activity of preventing any kind of serious crimes especially those committed in digital area;
- analyzing the storing device and digital system which contain digital traces;
- defining new terms and expressions used by both legislation and doctrine which lead to digital new means of technologies;
- establishing conclusive remarks on the procedure of using new means of technologies in criminal proceedings;

5. In practice, there were several cases in which the judicial bodies administered evidence gathered illegally by the other administrative bodies than the judicial investigative ones. In these cases, the count of law rejected them and pronounced the judicial decision exclusively based on the legal evidence administered as well: Penal Decision no. 18/ 15.02.2017 of the Iasi Court of Law, available online <http://portal.just.ro> (accessed 14.12.2019); Preliminary Penal Decision no. 31/C/ 27.09.2018 of the High Court of Cassation and Decision of Romania, available online <https://www.scj.ro> (accessed 14.12.2019).

- proposing a set of *de lege ferenda* proposals which must be taken into account by the legislator in the procedure of improving legislation in criminal matters into force.

METHODOLOGY OF RESEARCH

In reaching the proposed aims, the paper approaches a methodology of research, as pointed out below.

The current paper is based on a qualitative research study carried out on the most relevant elements the digital world provides the investigation bodies with. It is designed by a more comprehensive analysis and synthesis in a conceptual context the research paper is featured with.

In achieving the proposed aims, a mixed method of research has been used which consists in an in-depth research on the main aspects related to finding digital ways and tools of gathering digital evidence as well as approaching standardization of digital means of procedure used in criminal proceedings.

Taking into account all these aspects related above, the paper does neither use data gathered from both public institutions and private organizations, nor generate such data, due to the fact that it is not an empirical research.

Nevertheless, the paper approaches certain jurisprudence aspects in case-law pronounced in practice by the courts of law whose judicial decisions have been adopted through the use of digital evidence and scientific techniques.

Moreover, doctrine has permanently been involved in improving the issues regarding the new means of technologies and their use in criminal proceedings, both in the investigation and judgment phases. Several authors are currently involved in conducting research on this topic whose research conclusions, well-known at the international level, highlight a great value in the field. Their research results will be a conclusive basis for the current research project.

Last, but not least, infringing the parties' rights during the penal proceedings is a serious drawback which must be sanctioned by the law enforcement. The legislator must also take it into consideration in order to enhance the legal framework in accordance with both the home legislation in criminal matters and the European one, adopted by the EU institutions which is compulsory for the Member States.

ACHIEVEMENTS AND FAILURES THROUGH USING NEW TECHNOLOGIES

General background

The procedure of using new means of technologies has permanently been in both practitioners and theorists' attention who have investigated the aspects related to the criminal procedures achieved by means of new technologies. Solving penal cases having as

object crimes committed in a digital environment is the main target of the courts of law. In order for the judicial bodies to reach this goal and pronounce the legal and justified judicial decision, a set of judicial instruments has been activated. These instruments, also called as "smart technologies"⁶, are used by the investigation bodies during the investigation phase of penal proceedings, as well as by the judges during the judgment phase of penal trial.

The legal framework in this matter is structured around the provisions of Article 138-153 Code of penal procedure of Romania. The judicial instruments regarding the special measures of surveillance and investigation used in criminal matters are regulated in accordance with the presumption of innocence⁷ and the European principle of fair trial⁸. This means that ensuring the criminal proceedings must be viewed as a form of enhancing fair trial⁹.

Taking into account these provisions, the legislator has referred to the following special methods of surveillance and investigation:

- intercepting communications or any other kinds of communication at distance;
- accessing an information system;
- video/ audio/ photo surveillance;
- localizing and surveillance through technical device;
- gathering data on individuals' financial transactions;
- retaining, delivering and seizing postal correspondence;
- using undercover investigators and collaborators;
- authorized participation in certain activities;
- supervised delivery;
- gathering trafficking and localizing data processed by the contractors of public networks of electronic communications.

The use of artificial intelligence technology is at the moment a new concept and element of fair trial in court proceedings under protection of Article 6 of the European

6. Lupo, G., Velicogna, M., "Making EU justice smart? Looking into the implementation of new technologies to improve the efficiency of cross border justice services delivery", in *M. P. Rodriguez, Smart Technologies for Smart Governments*, Springer International Publishing, 2018, pp. 95-121.

7. Flynn, A., Hodgson, J., McCulloch, J., Naylor, B., "Legal aid and access to legal representation: redefining the right to a fair trial", in *Melbourn University Law Review*, 2016, 40(207), pp. 207-239; Hudson, G., "Secret hearings and the right to a fair trial", in *Canadian Human Rights Yearbook*, 2017, available online at: <https://ssrn.com/abstract=2897228> (accessed on 31.01.202).

8. Heikkinen, T. H., "How does the use of artificial intelligence affect the concept of fair trial?", 2019. Available online at: <http://lup.lub.lu.se/student-papers/record/8980709> (accessed on 01.02.2020); Dimovski, D., Pesic, P., "Ude of evidence obtained in breach of the Convention Rights as a violation of the rights to a fair trial", *Facta Universitatis, Law and Politics*, 2017, 15(3), pp. 181-190. <https://doi.org/10.22190/FULP1703181D>

9. Gless, S., Richter, T., "Do exclusionary rules ensure a fair trial? A comparative perspective on evidentiary rules", *Cham: Springer*, 2019, pp. 17-24.

Convention on Human Rights¹⁰. The Court also protects the parties' rights during the criminal proceedings, for all categories of serious crimes, including those committed in a digital context¹¹.

Constitutional prevalence in criminal proceedings

The activities conducted during the investigation phase of penal proceedings are set up in accordance with the juridical architecture of the entire legal principles which feature them. For this reason, speaking and analyzing the constitutional principles appear as a well-required element for the justice in criminal matters, whose inobservance would conclude in rejecting investigation activity by the court of law.

All actions ordered and carried out in the field of criminal matters are regulated and practiced in accordance with the principle of respecting the individual's private life and its integrity both physical and its property, as the principle is regulated by the constitutional provisions¹². Even if certain judicial actions are carried out through infringing the individual's private life, they are more accustomed to the idea of respecting the other principles the legislation into force also regulates in the matter of investigating and solving penal cases through genuine evidence, gathered by the judicial bodies under legality condition.

It is considered that any interference of the judiciary in the private life of individuals is necessary as long time as it respects their both procedural and constitutional rights. Actually, in this matter, only a limitation of their constitutional rights operates with the authorization ordered by the judge.

In this legal framework, some defining terms and expressions used by the judicial bodies are explained in purpose to prevent encroachments in the individual's private life. For this reason, intercepting communications is considered as being accessing, supervising, gathering and recording phone communications or any other activity carried out through a digital system or another mean of communication.

10. *Ibidem*.

11. Regarding the Case of Bucur and Toma c. Romania, the ECtHR stated that "In the case of a 'whistle-blower' who had revealed unlawful secret surveillance, the Court considered that civil society was directly affected by the information disclosed, for anybody could have his or her telephone tapped. Furthermore, this information being connected to abuses committed by high-ranking officials and affecting the democratic foundations of the State, those were very important issues which were matter for political debate, and which the public had a legitimate interest in being told about", in European Court of Human Rights. Research Division, National Security and European case-law, 2013, available online at: https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf (accessed on 22.01.2020).

12. Article 26 of the Constitution of Romania, republished in the Official Journal of Romania, no. 669 of 22 September 2003. Alonzi, F., „L'escalation dei mezzi di intrusione nella sfera privata: repartire dalla Costituzione”, *Revista Brasileira de Direito Processual Penal*, 2019, 5(3), pp. 1421-1448. Available online <http://www.ibraspp.com.br/revista/index.php/RBDPP/issue/view/11> (accessed 20.12.2019).

Doctrine has stated that "To minimize the problems (...) the admission of illegally obtained evidence should only be considered if other interests such as the accused's individual rights do not disproportionately outweigh the public interest in fighting crime"¹³.

The judicial system in criminal matters of Romania has also been involved in serious problems occurred through the use of illegal means of gathering evidence by another state body than the investigation one. In this case, the judge of preliminary court has stated¹⁴ that the defendants have been sent to trial of having committed the organized crime activities, incriminated by Article 367 (1) and (2) Penal Code of Romania. The *criminal activity* has consisted in trafficking in human beings, provided by Article 211 (1) and (2) Penal Code, and trafficking in persons by Article 210 (1/a and 1/b) Penal Code. The defendants invoked the exception of indictment illegality, arguing that "it is illegal from the point of view of the incriminated crimes provided by the prosecutor, as well as its conformity with the procedural acts carried out during the investigation phase"¹⁵. Regarding the illegality of administered evidence in the penal case, the defendant also required to the preliminary court's judge to give the case back to the investigation phase of penal proceedings, on the one hand, and order the nullity of communications interception reports, on the other hand. In accordance with these requirements, the defendant has argued that the procedure activities of investigation were carried out by the Romanian Services of Intelligence, and, for this reason, the legal judicial sanction which must be applied is the nullity, as stated by the Constitutional Court of Romania in Decision no. 51 of 2016¹⁶.

From a procedural point of view, the investigation activity including the defendant's surveillance by digital means and intercepting communications can also be ordered by the judge, but in the penal case they have been carried out by another state body than the investigation one¹⁷. This means that the evidence gathered through means of technology are null absolutely and must imperatively be removed from the penal case.

The penal procedure is featured by principle of legality and faithful of administering evidence during the investigation phase, which concludes in the sanction of nullity of those evidence gathered illegally. As a consequence, the reports of technical surveillance are declared under the provisions of the Constitutional Court decision concerning the procedural acts carried out by another state body than the investigation one. In this

13. Macula, L., „The potential to secure a fair trial through evidence exclusion: A Swiss perspective”, *Ius Gentium: Comparative Perspectives on Law and Justice*, vol. 74, in Gless, S., Richter, T., „Do exclusionary rules ensure a fair trial?” A comparative perspective on evidentiary rules, *op. cit.*, p. 39.

14. Iasi Court of Law, Penal Decision no. 18 of 15 February 2017, available online at: <http://portal.just.ro> (accessed on 18 September 2019).

15. *Ibidem*.

16. Constitutional Court Decision no. 51 of 2016 regarding the exception of unconstitutionality of Article 142 (1) Code of penal procedure of Romania, published in the Official Journal no. 190 of 14 March 2016.

17. Magherescu, D., „Using new means of technology during the penal proceedings in Romania”, *Revista Brasileira de Direito Processual Penal*, Porto Alegre, 2019, 5(3), pp. 1189-1217. <http://doi.org/10.22197/rbdpp.v5i3.250>

case, the preliminary court judge has stated that “the defendant indicated in concrete neither the material act of illegal interception, nor the kind of nullity which would affect the reports of communications interception, as provided by Decision no. 51 of 2016 of the Constitutional Court of Romania, they are prevailed of”¹⁸.

In accordance with the provisions stated by the Constitutional Court of Romania, which declare unconstitutionality of Article 142 (1) Code of penal procedure of Romania, the judicial activity of investigation in criminal cases, including defendant’s technical surveillance, may exclusively be carried out by the judicial bodies, especially designed by Article 142 thereof. They refer to the specialized investigation bodies.

Moreover, from a constitutional point of view, the Decision no. 51 of 2016 of the Constitutional Court of Romania has admitted the exception of unconstitutionality¹⁹ and stated that the expression „ either... or by the other specialized bodies of state...” regulated by Article 142 (1) Code of penal procedure of Romania is unconstitutional.

Taking into account this provision of the Constitutional Court, it is obviously that in the penal cases in which judicial bodies administered digital evidence gathered by the other state specialized bodies, the legal provisions on carrying out technical surveillance measures were infringed, because these activities have been achieved by an administrative body which does not have competence in carrying out activity of penal investigation. For this reason, the legal provisions on material competence in criminal matters were infringed, as argued above.

Infringing the rules of penal procedure which regulate the material competence in cases of carrying out the technical surveillance measures ordered by the judge is sanctioned with the absolute nullity. Thus, in conformity with the Constitutional Court Decision no. 302 of 2017²⁰, the nonobservance of provisions of the investigation body’s capacity is sanctioned with the absolute nullity, its effects being regulated by Article 281 Code of penal procedure of Romania.

Terminological view

The evolution of judicial activities, carried out in digital environment, has imposed the use of new collocations, came to meet the science and technical progress currently at a high interest in criminal matters, especially in serious cases, investigated by means of

18. Iasi Court of Law, Penal Decision no. 18 of 15 February 2017, available online at: <http://portal.just.ro> (accessed on 18 September 2019).

19. Constitutional Court Decision no. 51 of 16 February 2016, published in the Official Journal of Romania no. 190 of 14 March 2016.

20. The Constitutional Court of Romania has admitted the exception of unconstitutionality on the provisions of Article 281 (1/ b) Code of penal procedure of Romania which regulate the material and personal competence of the courts of law in criminal matters. The Court has motivated that “the legislative solution regulated by Article 281 (1/ b) thereof which does not regulate the absolute nullity for the procedure of infringing provisions regarding the material and personal competence of the investigation bodies is unconstitutional”. See in this matter, The Constitutional Court Decision no. 302 of 2017, published in the Official Journal of Romania no. 566 of 17 July 2017.

forensic science²¹. Thus, it is appreciated that "efficiency of the investigations carried out by the judicial bodies depends very frequently on the investigative techniques they are featured with"²².

For a better understanding the "language" of new technologies, used in penal cases, both legislator and doctrine have had an important contribution. Their attention were focused on terms and expressions as 'new entry' in the field of forensic investigation of particular cases of crimes, especially serious ones. In this context, a new era of digital technology has been opened, and a new technological approach of phenomenon has been arisen. Moreover, the available definitions are those stated by doctrine and legislation in criminal matters, most of them being related to digital system, digital evidence, digital data, forensic investigation, cybercrime, a.s.o.²³.

From terminological point of view, accessing digital system is commonly defined as penetrating a digital system or a mean of stoking digital data, either direct or at a distance, through specializing programs or network in purpose to identify evidence²⁴.

In both cases, a digital system that can be accessed by the judicial bodies during penal proceedings is a device or many ones connected each other which assure processing data automatically by using a digital program, as it is regulated by Article 138 (4) Code of penal procedure of Romania.

Digital data is also a new item used in criminal matters, which helps the judicial bodies in gathering digital evidence necessary for solving penal cases. They refer to the facts, information or concepts provided under an appropriate form of processing in a digital system, including a program able to determine drawing up a function by a digital system²⁵.

In the field of forensic investigation, the judicial situation is more particularly connected to the judicial bodies' activity, achieved under principle of efficiency and rapidity in gathering forensic evidence. They are frequently confronted with serious traps due to the fact that, most of the time, the criminals are accustomed to digital environment too²⁶.

Moreover, the concept of forensic investigation leads with forensic evidence, which means by law those evidence gathered by the forensic investigation bodies from the crime scene, analyzed and investigated scientifically through means provided in criminal matters. Doctrine has pointed out that the evidence have a double feature, which mean an instrument of knowledge, on the one hand, and they conclude in the existence or

21. Stancu, E., *Tratat de criminalistica*, Bucharest: Actami Publishing House, 2001.

22. Covalciuc, I., „Noi tehnici de investigatie: prevederi normative si posibilitati practice”, *Revista de Criminologie, Criminalistica si Penologie*, 2019, 4, p. 67.

23. *Ibidem*.

24. Gehl, R., Plecas, D., *Introduction to criminal investigation: processes, practices and thinking*, New Westminster: Justice Institute of British Columbia, 2016, pp. 151-152.

25. According to Article 138 (5) Code of penal procedure of Romania, adopted by Law no. 135 of 2010 published in the Official Journal of Romania no. 486 of 15 July 2010, into force from 1 February 2014.

26. Casey, E., *op. cit.*, pp. 10-13.

inexistence of crime, on the other hand²⁷. Generally speaking, the forensic evidence are defined as extra-procedural entities, which refer to the criminal action and perpetrator, suspected of having committed a crime, whose administration during the criminal proceedings, either in the investigation phase or in judgment phase, assert them a procedural character²⁸.

Last but not least, the encroachments in the individual's private life is also related to the issue of personal data protection in criminal proceedings²⁹, especially when using them as investigation material and pre-constitutional probative accusation³⁰. This argument is based prevalently on the idea of an inseparable relation between the constitutional provisions and the penal procedure ones³¹.

The digital environment of a person is also under protection of both the constitutional and procedural principles, which state that the law guarantees the person's inviolability of domicile and its online activity, as private one. In this regard, the law enforcement agencies have to consider the persons' private activities carried out either at home and in digital context. Otherwise, they can be infringed and some encroachments are allowed by the judge in particular cases expressly regulated by the Code of penal procedure.

DOCTRINAL AND JURISPRUDENCE APPROACH

The main discussion of the current paper is focused around the idea of the efficiency of new means of technologies, used in criminal proceedings in order to prevent any kind of criminality, including serious crimes³², from homicides to trafficking, from corruption to terrorism. At present, digital forensic science has reached a high level of development, a "profession and scientific discipline has its roots in the efforts of law enforcement to address the growth in computer-related crime"³³.

From a theoretical point of view, the influence of new technologies in criminal proceedings is highly approached by doctrine. It is considered as being a core relation be-

27. Covalciuc, I., *op. cit.*, p. 71.

28. *Ibidem*.

29. González Cano, I., „Cesión y tratamientos de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680”, en *Revista Brasileira de Direito Processual Penal*, 2019, 5(3), pp. 1331-1384. <https://doi.org/10.221.97/rbdpp.v5i3.279>

30. *Ibidem*.

31. Alonzi, F., *op. cit.*, pp. 1422-1425.

32. Mastronardi, V., Neri, G., „Serial murders: Criminological profiles”, in *Rivista di Psicopatologia Forense, Medicina Legale, Criminologia*, 2017, 22, pp. 22-26; Swig, D. L., *Domestic violence response: video recording initial statements to increase prosecution rates*, West Sacramento, 2010, p. 4.

33. Casey, E., *Digital evidence and computer crime*, *op. cit.*, p. 10. In the last decade, the law enforcement officials of the USA started working in close cooperation in purpose to enhance their professional activity and institutional capacity to deal with particular cases. It consists in training courses and programs organized in centers and institutes of research, most frequent used being the Federal Law Enforcement Center and National White Collar Crime Center.

tween the digital evidence and computer crime³⁴, even if it is not limited to the last one. Actually, more crimes could be committed in a digital context, including banking area, child pornography on computer a.s.o., which particularly mean the involvement of forensic science, computers and the internet³⁵.

In practice, the techniques and methods used in order to gather evidence is discussed under principle of certainty. In this regard, it has been appreciated that "In Forensic Science, *certainty* is a word that is used with great care. We cannot be certain of that occurred at a crime scene when we only have a limited amount of information. Therefore, we can generally only present possibilities based on the limited amount of information"³⁶. In this context, doctrine advances the idea of increasing awareness of digital evidence.

On the large number of criminal phenomena, particular attention being paid on the serious forms of criminality and organized crimes committed in a transnational feature³⁷, the law enforcement has reacted in finding new legal ways more efficient to combat them. Enhancing procedure of using new means of technologies in criminal proceedings has transcended in an imperative tool of achieving justice in criminal matters. This is because the criminal cases investigated and judged by the judicial bodies are solved in a spread area, which involves not just classical judicial instruments, but more comprehensive ones.

From a practical point of view, it is of high interest how digital data is transposed in a material evidence as well as how judicial bodies must provide the original digital evidence. The first issue comes to analyse digital evidence in technical manner, while the second in an organizational one. In fact, by printing digital data, very important information on the circumstances the crime was committed in will be lost. The procedure involves especially metadata which will be displayed from folder.

From a formal point of view, the information contained through digital evidence will also be lost, due to the fact that the code provided by folder depends on the IT program and its version the forensic experts use in gathering such data. In this context, it is well-known that printing a digital data is not equivalent with the original pattern.

Doctrine has discussed about the procedure of recognizing the quality of document for a private person's correspondence which may be used during the penal proceedings as an evidence³⁸. It is provided in accordance with Article 198 Code of penal procedure. Instead, there is no legal provision to regulate how judicial bodies can administer the evidence on digital correspondence of a person³⁹.

34. Casey, E., Digital evidence and computer crime, *op. cit.*, pp. 10-13.

35. *Ibidem*.

36. *Idem*, p. 14.

37. Magherescu, D., „Particularities of the forensic science investigation of transnational serious crimes”, in *Ius et Scientia*, 2019, 5(2), pp. 55-75. <http://doi.org/10.12795/IESTSCIENTIA.2019.i02.04>

38. Suian, M., „Unele probleme privind folosirea probelor digitale in procesul penal”, in *Doctrina si Jurisprudenta*, 2019, 1, pp. 134-141.

39. *Ibidem*.

Jurisprudentially speaking, the procedure of administering evidence of printing e-mail messages sent and/ or received by a person is frequently met in practice. Nevertheless, parties do not take into account the cases in which such method of printing digital evidence does not preserve the evidence entirely. It is more an abstractization of a real evidence administered through a method which permits parties to prove what exactly has been sent or received in a digital context. For this reason, the other parties involved in criminal proceedings can require the judge to either administer a counter evidence or remove it.

Although there is no an imperative provision regulated in this matter by the Code of penal procedure of Romania, the jurisprudence is so confident with the procedure of transposing digital evidence in a printing form, more specifically once the new Code of penal procedure of Romania entered into force on the 1st of January 2014⁴⁰.

CONCLUSION

Using the methodology of research which fits better with the topic proposed by the current paper on enhancing procedure of using new means of technologies in criminal proceedings, the aspects provided have been analyzed and discussed in such a manner to achieve the objectives stated in the the beginning of research. The conclusive section highlights the most appropriate results that have been gathered during the research study. They point out that the most recent digital means of technologies used by the investigation bodies during the judicial activity are so necessary in a spread area of digital criminal environment.

The current research concludes that the legislation in criminal procedure law into force has a series of lacks whose improvement is necessary in order for the judicial bodies to achieve the goals of their both investigation and judgment activities. In this matter, the legislation must be amended as much as possible in accordance with the European one, due to the Romania's status as a Member State of the European Union.

At present, using new means of technologies, including digital and forensic ones, has produced consequences in the field of enhancing process of solving criminal cases.

De Lege Ferenda Proposal

In accordance with the conclusions pointed out above, the remarks must be followed by a *de lege ferenda* proposal, whose solutions could be taken into consideration by the legislator in the legislative process of improving the legal framework in criminal matters, in particular referring to the criminal cases which are investigated and solved through digital evidence.

40. Law no. 135 of 2010 on the Code of penal procedure of Romania, published in the Official Journal of Romania no. 486 of 15 July 2010, into force from 1 February 2014.

Using new means of gathering digital evidence, in digital environment, is an efficient activity the judicial bodies are looking for improving it in order to achieve the best results in their activity of investigation in such a way to diminish or destroy criminal groups, which commit digital crimes.

Moreover, the current legislation in criminal matters must be modified in conformity with the social changes and technological ones too. Developing technology in the 21st century has created premises for the virtual world, which has the merit of transposing real actions through the information technology systems.

Despite these features, the law is sometimes outdated of digital evidence and practical solutions in this area as well as of the future issues. They are more subordinated to the principle of legality in the field of administering digital evidence, and investigating the crime scene in a digital context.

Acknowledgement

I would like to express my thanks to the *Ius et Scientia's* Editorial Board and anonymous reviewers who accepted my article for publication in the next issue of journal. It is the result of my own research work, carried out during one year-period, started in the beginning of 2019. There is no financial source provided for its publishing process.

Conflict of interest

There is no conflict of interest related to the paper published.

BIBLIOGRAPHY

- Alonzi, F., L'escalation dei mezzi di intrusione nella sfera privata: repartire dalla Costituzione, *Revista Brasileira de Direito Processual Penal*, 2019, 5(3), pp. 1421-1448. Available online <http://www.ibraspp.com.br/revista/index.php/RBDPP/issue/view/11> (accessed 20.12.2019)
- Casey, E., *Digital evidence and computer crime*. Third Ed., Elsevier, Maryland, 2011.
- Code of penal procedure of Romania, adopted by Law no. 135 of 2010 published in the Official Journal of Romania no. 486 of 15 July 2010, into force from 1 February 2014.
- Constitution of Romania, republished in the Official Journal of Romania, no. 669 of 22 September 2003.
- Constitutional Court Decision no. 51 of 16 February 2016, published in the Official Journal of Romania no. 190 of 14 March 2016.
- Covalciuc, I., Noi tehnici de investigatie: prevederi normative si posibilitati practice, *Revista de Criminologie, Criminalistica si Penologie*, 2019 (4), pp. 67-74.
- Dimovski, D., Pesic, P., Use of evidence obtained in breach of the Convention Rights as a violation of the rights to a fair trial, *Facta Universitatis, Law and Politics*, 2017, 15(3), pp. 181-190. <https://doi.org/10.22190/FULP1703181D>

- Dzehtsiarou, K., European Consensus and the Evolutive Interpretation of the European Convention on Human Rights, *German Law Journal*, 2011, 12(10), pp. 1730-1745. <https://doi.org/10.1017/S2071832200017533>
- European Convention on Human Rights of 1950, entered into force in 1953, Council of Europe, Cedex, Strasbourg, available online at: https://www.echr.coe.int/Documents/Convention_ENG.pdf (accessed on 02.11.2019)
- European Court of Human Rights. Research Division, National Security and European case-law, 2013, available online at: https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf (accessed on 22.01.2020)
- Flynn, A., Hodgson, J., McCulloch, J., Naylor, B., Legal aid and access to legal representation: re-defining the right to a fair trial, *Melbourn University Law Review*, 2016, 40(207), pp. 207-239.
- Gehl, R., Plecas, D., Introduction to criminal investigation: processes, practices and thinking, Justice Institute of British Columbia, New Westminster, 2016.
- Gless, S., Richter, T., Do exclusionary rules ensure a fair trial? A comparative perspective on evidentiary rules, Springer, Cham, 2019.
- González Cano, I., Cesión y tratamientos de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680, *Revista Brasileira de Direito Processual Penal*, 2019, 5(3), pp. 1331-1384. <https://doi.org/10.221.97/rbdpp.v5i3.279>
- Heikkinen, T. H., How does the use of artificial intelligence affect the concept of fair trial?, 2019. Available online at: <http://lup.lub.lu.se/student-papers/record/8980709> (accessed on 01.02.2019)
- Hudson, G., Secret hearings and the right to a fair trial, *Canadian Human Rights Yearbook*, 2017, available online at: <https://ssrn.com/abstract=2897228> (accessed on 31.01.2020)
- Lupo, G., Velicogna, M., Making EU justice smart? Looking into the implementation of new technologies to improve the efficiency of cross border justice services delivery, in M. P. Rodriguez, *Smart Technologies for Smart Governments*, Springer International Publishing, 2018, pp. 95-121.
- Macula, L., The potential to secure a fair trial through evidence exclusion: A Swiss perspective, *Ius Gentium: Comparative Perspectives on Law and Justice*, Springer, 2019, vol. 74.
- Magherescu, D., Particularities of the forensic science investigation of transnational serious crimes, *Ius et Scientia*, 2019, 5(2), pp. 55-75. <http://doi.org/10.12795/IESTSCIENTIA.2019.i02.04>
- Magherescu, D., Using new means of technology during the penal proceedings in Romania, *Revista Brasileira de Direito Processual Penal*, Porto Alegre, 2019, 5(3), pp. 1189-1217. <http://doi.org/10.22197/rbdpp.v5i3.250>
- Mastronardi, V., Neri, G., Serial murders: Criminological profiles, *Rivista di Psicopatologia Forense, Medicina Legale, Criminologia*, 2017, vol. 22, pp. 22-26.
- Penal Decision no. 18 of 15 February 2017 of the Iasi Court of Law, available online <http://portal.just.ro> (accessed 14.09.2019)
- Preliminary Penal Decision no. 31/C/ 27.09.2018 of the High Court of Cassation and Decision of Romania, available online <https://www.scj.ro> (accessed 14.12.2019)
- Stancu, E., *Tratat de criminalistica*, Actami Publishing House, Bucharest, 2001.
- Suian, M., Unele probleme privind folosirea probelor digitale in procesul penal, *Doctrina si Jurisprudenta*, 2019, 1, pp. 134-141.
- Swig, D. L., Domestic violence response: video recording initial statements to increase prosecution rates, West Sacramento, 2010.