

THE ADVERSARIAL SYSTEM IN THE CRIMINAL PROCESS OF UKRAINE: TECHNICAL AND LEGAL ASPECTS

ANTON STOLITNII,
Classical Private University (Zaporizhia, Ukraine)

DOI: 10.17589/2309-8678-2019-7-1-154-177

This article substantiates the author's scientific concept of electronic criminal proceedings, as regards the use thereof in the adversarial system, which would involve the formation of criminal proceedings as an electronic file, and the procedural interaction of the subjects of proceedings in an electronic law enforcement environment. The tasks of this article are as follows: analysis of issues that may arise when establishing such adversarial system in the criminal process of Ukraine; study of foreign experience of involving a defense lawyer in electronic criminal procedural processes; and development of proposals for improving the domestic practice of law enforcement.

The Uniform Register of Pre-trial Investigations (URPI) has been defined as an electronic procedural document and an integral segment of criminal proceedings. The analysis of the electronic segment of the pre-trial investigation shows that the lawyer's procedural status needs to be improved by his/her involvement in the URPI. Based on the analysis of the experience of electronic criminal proceedings in the province of Alberta (Canada), the Czech Republic, Sweden, and Kazakhstan, proposals have been drawn up to bring the defense to the URPI.

As a result of the study, the author identified the legal and technical aspects of involving an attorney in electronic criminal proceedings, which suggested successive practical steps in creating personal virtual accounts, an algorithm for involving a defense lawyer in proceedings, and reforming the Uniform Register of Lawyers of Ukraine (URLU) as an electronic procedural legalization instrument.

Keywords: Ukraine; electronic criminal proceedings; adversarial system; electronic procedural document; electronic law environment; cybersecurity.

Recommended citation: Anton Stolitnii, *The Adversarial System in the Criminal Process of Ukraine: Technical and Legal Aspects*, 7(1) Russian Law Journal 154–177 (2019).

Introduction

The reform of criminal justice in Ukraine has brought about qualitative changes in the nature of the implementation of criminal procedural activities. With the introduction of the *Unified Register of Pre-trial Investigations* (hereinafter the *URPI* or the *Register*), an electronic segment of the criminal process was created that legally (procedurally) and technically is an integral part of the *Register*. It predetermines certain activities of the subjects of criminal proceedings in the electronic law enforcement environment.

According to Article 7 of the *Criminal Procedural Code of Ukraine* (hereinafter the *CPC of Ukraine*), the adversarial system should be used in criminal proceedings.¹ One of the key features of the adversarial system is enshrined by the legislator in the definition of the concept of the criminal proceedings' parties. In accordance with para. 19 of part 1 of Article 3 *CPC of Ukraine*, the parties to criminal proceedings are: for the prosecution, an investigator, the head of the pre-trial investigation body, the prosecutor, as well as the victim, his/her representative and a legal representative in cases specified by the *CPC of Ukraine*; and, for the defense, the suspect, the accused (defendant), convicted or acquitted person, a person for whom the use of compulsory measures of a medical or educational nature is foreseen, or for whom the matter of their use has been resolved, their defense and legal representatives. Their rights in the electronic segment are not the same, since the prosecution party has exclusive powers of full access to the *URPI*, while the defense parties do not have direct access to the *Register*.

Therefore, the restriction of the defense's access to the information of the electronic segment of the criminal process is not compliant with the adversarial system, which is a problem both for the science of the criminal process of Ukraine and for the practice of law enforcement, therefore, it requires further research.

Various aspects of the adversarial system are the subject of numerous studies by Ukrainian scholars. The theoretical aspects of this issue were studied by K. Lysenkova,² M. Markush,³ M. Nozdrina⁴ and others.

¹ Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI [Criminal Procedural Code of Ukraine No. 4651-VI of 13 April 2012] (Feb. 12, 2019), available at <https://zakon.rada.gov.ua/laws/show/4651-17>.

² See Лисенкова К. Правова сутність змагальності в кримінальному провадженні // Юридичний вісник. 2014. № 4. С. 334–337 [Kira Lysenkova, *The Legal Essence of the Adversarial System in Criminal Proceedings*, 4 Legal Bulletin 334 (2014)].

³ See Маркуш М.А. Феномен змагальності та конституційно-правова модель змагальності у кримінальному процесі України // Наукові записки Інституту законодавства Верховної Ради України. 2016. № 2. С. 63–69 [Maria A. Markush, *The Adversarial System and Its Constitutional and Legal Model in the Criminal Process of Ukraine*, 2 Scientific Notes of the Institute of Legislation of the Verkhovna Rada of Ukraine 63 (2016)].

⁴ See Ноздріна М.О. Диспозитивність як елемент принципу змагальності у кримінальному процесі України: Автореф. дис. ... канд. юрид. наук [Marina O. Nozdrina, *Dispositivity as an Element of the*

V. Tertyshnyk investigated the status of a defense lawyer in the adversarial criminal process.⁵ A. Biriukova and M. Ostrovska analyze issues affecting the adversarial system in different states and compare them with the practice of enforcement in Ukraine.⁶ A. Pritula considers adversity as a prerequisite for a fair trial.⁷ O. Tolochko, V. Jurchishin and O. Janovska highlight the law-implementation aspect of this issue.⁸

It is worth noting that S. Martynova developed the theoretical and applied problems of the adversarial system.⁹ S. Darovskikh studied the mechanism of the implementation of this principle.¹⁰ R. Bagdasarov analyzed the adversarial process in the criminal process of the Russian Federation and the states of the European Union.¹¹ I. Sotsaniuk studied the adversarial system in the criminal process of the Kyrgyz Republic in a dissertation study.¹²

Adversarial System in the Criminal Process of Ukraine: Abstract of a Law PhD Thesis] (Kharkiv: National University of Internal Affairs, 2004); *Строгович М.С. Природа советского уголовного процесса и принцип состязательности* [Mikhail S. Strogovich, *The Nature of the Soviet Criminal Process and the Adversarial System*] (Moscow: NKU of the USSR, 1939).

⁵ *Тертишник В.М.* Захисник у змагальному кримінальному процесі // Бюлетень Міністерства юстиції України. 2010. № 12. С. 90–95 [Volodimir M. Tertyshnyk, *Defense Lawyer in an Adversarial Criminal Process*, 12 Bulletin of the Ministry of Justice of Ukraine 90 (2010)].

⁶ *See Бірюкова А.М., Островська М.А.* Модель змагальності за проектом Кримінального процесуального кодексу України (у порівнянні з іншими країнами світу) // Адвокат. 2012. № 4. С. 12–16 [Alina M. Biriukova & Maria A. Ostrovska, *Competition Model Under the Draft Criminal Procedure Code of Ukraine (in Comparison with Other Countries of the World)*, 4 Lawyer 12 (2012)].

⁷ *Притула А.М.* Змагальність у кримінальному процесі як передумова справедливого суду // Юридична наука. 2014. № 8. С. 117–122 [Anatolii M. Pritula, *Competition in the Criminal Process as a Prerequisite for a Fair Trial*, 8 Legal Science 117 (2014)].

⁸ *See Толочко О.* Реалізація принципу змагальності під час досудового розслідування // Вісник Національної академії прокуратури України. 2014. № 2(35). С. 59–65 [Oleksandr Tolochko, *Implementation of the Adversarial System During the Pre-Trial Investigation*, 2(35) Bulletin of the National Academy of the Public Prosecutor of Ukraine 59 (2014)].

⁹ *Мартынова С.И.* Состязательность сторон на досудебной стадии уголовного процесса: теоретико-прикладные проблемы // Адвокат. 2011. № 4. С. 25–28 [Svetlana I. Martynova, *Adversarial System at the Pre-Trial Stage of the Criminal Process: Theoretical and Applied Problems*, 4 Lawyer 25 (2011)].

¹⁰ *Даровских С.М.* Принцип состязательности в уголовном процессе России и механизм его реализации: Автореф. дис. ... канд. юрид. наук [Svetlana M. Darovskikh, *Adversarial System in the Criminal Process of Russia and the Mechanism for Its Implementation: Abstract of a Law PhD Thesis*] (Chelyabinsk: South Ural State University, 2001).

¹¹ *Багдасаров Р.В.* Принцип состязательности в уголовном процессе России и стран Европейского Союза [Roman V. Bagdasarov, *Adversarial System in the Criminal Process in Russia and the European Union*] (Moscow: Yurlitinform, 2008).

¹² *Соцаниук И.Ю.* Состязательность в уголовном процессе Кыргызской Республики: Автореф. дис. ... канд. юрид. наук [Ivan Yu. Sotsaniuk, *Adversarial System in the Criminal Process of the Kyrgyz Republic: Abstract of a Law PhD Thesis*] (St. Petersburg: St. Petersburg University of the Ministry of Internal Affairs of Russia, 2011).

A study by D. Epps of competitive asymmetry in the work of prosecutors in the United States should also be taken into account.¹³ J. Langbein gives a very relevant explanation of the origins of the adversarial criminal process, a detailed and innovative study of the most distinguishing feature of the Anglo-American legal systems.¹⁴

K. Findley analyzes alternative methods of investigating and resolving criminal cases in relation to the relative advantages of inquisitorial and adversarial systems.¹⁵

K. MeUlli investigated the prosecution's discretion in the U.S. adversarial system, in particular, the prosecution's function from the prosecutor's point of view.¹⁶ J. Ainsworth compares the competitive and inquisitorial model and concludes that, in many countries which traditionally use inquisitorial processes, more competitive models of evidence presentation have been used in court sessions, which has strengthened the position of lawyers.¹⁷

L. Rusu considers the principle of adversity through the prism of the criminal process in Moldova, i.e. the degree of implementation, its essence, the problems of its implementation within different stages of the criminal process, aspects of comparative law, etc.¹⁸ This study allowed the specification and development of the adversarial system's conceptual framework, and the drafting of recommendations on the improvement of criminal-procedural legislation and the necessity of initiating and conducting a study of the adversarial system within the framework of criminal-procedural activity.

J. Ogg examines the nature and extent of competitive procedures in the criminal process in Italy and Austria, the combination of inquisitorial and adversarial elements in criminal proceedings of these states, which, in particular, have a significant impact on the subjects of the process.¹⁹

T. Kirchengast investigated the question of the establishment of a lawyer's institute representing the interests of victims in criminal proceedings in the

¹³ Daniel Epps, *Adversarial Asymmetry in the Criminal Process*, 4(91) New York University Law Review 762 (2016).

¹⁴ John H. Langbein, *The Origins of Adversary Criminal Trial* 354 (Oxford: Oxford University Press, 2003).

¹⁵ Keith A. Findley, *Adversarial Inquisitions: Rethinking the Search for Truth*, 56 New York Law School Law Review 911 (2011).

¹⁶ Kenneth J. MeUlli, *Prosecutorial Discretion in an Adversary System*, 1992(3) BYU Law Review 669 (1992).

¹⁷ Janet Ainsworth, *Legal Discourse and Legal Narratives: Adversarial Versus Inquisitorial Models*, 2(1) Language and Law – Linguagem e Direito 1 (2015).

¹⁸ Rusu Lucia, *Principiul contradictorialității în procesul penal – reglementări naționale și de drept comparat: Autoreferatul tezei de doctor în drept [The Principle of Contradictory in the Criminal Proceeding – National and Comparative Law Regulations: Abstract of a Law PhD Thesis]* (Feb. 12, 2019), available at http://www.cnaa.md/files/theses/2016/50736/lucia_rusu_thesis.pdf.

¹⁹ James T. Ogg, *Adversary and Adversity: Converging Adversarial and Inquisitorial Systems of Justice – a Case Study of the Italian Criminal Trial Reforms*, 37(1) International Journal of Comparative and Applied Criminal Justice 31 (2013).

system of adversarial criminal justice in England and Wales, the USA and Australia, compared with the positive experience of Sweden in this matter.²⁰ Swedish criminal investigations were studied by Swedish scholars such as A. Kornstrand who, however, do not promote the electronic aspect of the adversarial system due to the absence of the defense as a subject of the Swedish electronic procedural dialogue.²¹

Through the prism of electronic criminal proceedings, the adversarial system was not sufficiently studied in the domestic and foreign science of the criminal process.

I. Ilikchieva and A. Pavliuk analyzed the problems of the functioning of the *Uniform Register of Lawyers of Ukraine* (hereinafter the *URLU*), but not in the context of the potential procedural element of electronic criminal proceedings.²² Similarly, this aspect is not reflected in studies of the *URPI* (with the exception of the scientific works of the author of this article). In the science of the criminal process of Ukraine, the scientific school of electronic criminal proceedings is now at the stage of formation. The author has been developing a comprehensive concept in this direction for the last five years.²³ This study is one of the constituent elements of this concept.

The general tendency of the above-mentioned research is a thorough development of an adversarial system's theoretical and practical aspects in the criminal process, its improvement along with the simultaneous absence of analysis of the status of the procedural electronic segment. In turn, the study of the electronic component of the criminal proceedings illustrates significant gaps regarding the proper procedural electronic segment of the protection side and the potential introduction of an instrument of innovative law enforcement on its basis. Therefore, in the science of the criminal process, the issue of the technological aspect of the adversarial system as regards the electronic segment of criminal proceedings has simply not been investigated or even formulated, which is why this work is so relevant.

The subject of this study is the technical and legal components of the adversarial system in the criminal process of Ukraine and their improvement. The task of this work is to analyze the problem of the adversarial system in the criminal process of Ukraine, in particular, in the electronic law enforcement environment, the study of the foreign experience of involving the defense in electronic criminal procedures, and the formation of proposals on the improvement of domestic law enforcement practice on its basis.

²⁰ Tyrone Kirchengast, *Victim Lawyers, Victim Advocates, and the Adversarial Criminal Trial*, 16(4) *New Criminal Law Review* 568 (2013).

²¹ Agneta Kornstrand, *Informationshanteringen i rättskedjan*, 4 *Svensk Juristtidning* 556 (2009) (Feb. 12, 2019), also available at <http://svjt.se/svjt/2009/556>.

²² Ілікчієва К., Павлюк А. Єдиний реєстр адвокатів України: питання подальшого реформування // Юридичний вісник. 2014. № 3. С. 46–52 [Katerina Ilikchieva & Alena Pavliuk, *The Unified Register of Lawyers in Ukraine: Issues of Further Reform*, 3 *Legal Bulletin* 46 (2014)].

²³ Столітній А.В. Електронне кримінальне провадження: передумови виникнення, сучасний стан та перспективи розвитку [Anton V. Stolitnii, *Electronic Criminal Proceedings: Preconditions for the Emergence, Current State and Prospects of Development*] (Kyiv: Publishing house "ArtEk," 2016).

1. Methods

In the process of research, a complex of general scientific and special research methods was applied. The method of system analysis is used when comparing the electronic criminal procedural activities of different states.²⁴

The survey method was used when collecting legal information from specialized criminal proceedings (investigators, prosecutors, lawyers, investigators and judges) in relation to issues studied in the work.²⁵

The statistical method was used in the elaboration of the results of a survey conducted by the author on the subject.²⁶ The method of analogy was used in the study of the legal nature of the information of the electronic segment of criminal proceedings.²⁷

The comparative method was used to compare the norms of modern criminal procedural legislation of Ukraine with the normative regulation of criminal procedural activity in pre-trial proceedings of foreign countries.²⁸

The formal-legal method was applied to clarify the essence of the norms of domestic criminal procedural legislation, and in the development of proposals to improve it.²⁹ A modelling method was used in the design of an electronic dialogue system between specialized criminal proceedings.³⁰

The formal-dogmatic method was used in the study of legal concepts, the formal-logical analysis of the content of domestic and foreign legislation, and legal constructions on the subject.³¹ For the analysis and modeling of the algorithm of the functioning of the electronic segment of criminal proceedings in accordance with the adversarial system, a cybernetic method was used.³²

²⁴ Шаратов О.Д., Дербенцев В.Д., Семьонов Д.Е. Системний аналіз: Навч.-метод. посіб. для самост. вивч. дисц. [Oleksandr D. Sharapov et al., *System Analysis: A Manual for Independent Study of Discipline*] (Kyiv: Kyiv National University of Economics, 2003).

²⁵ Танчин І.З. Соціологія: Навчальний посібник [Igor Z. Tanchin, *Sociology: Study Guide*] (Kyiv: Znannia, 2008).

²⁶ Лисенков С.Л., Колодій А.М., Тихоміров О.Д., Ковальський В.С. Теорія держави і права: Підручник [Sergii L. Lysenkov et al., *Theory of State and Law. Study Guide*] 448 (Kyiv: Yurinkom Inter, 2005).

²⁷ Гусарев С.Д., Тихоміров О.Д. Юридична деонтологія [Stanislav D. Gusarev & Oleksandr D. Tikhomirov, *Legal Deontology*] 506 (Kyiv: VIRA-R, 1999).

²⁸ Крестовська Н.М., Матвеева Л.Г. Теорія держави і права: Елементарний курс [Natalia M. Krestovska & Liliya G. Matveeva, *Theory of State and Law: An Elementary Course*] 432 (Kharkiv: Odysei, 2008).

²⁹ Сухонос В.В. Теорія держави і права: Навч. посіб. [Volodimir V. Sukhonos, *Theory of State and Law: Study Guide*] 536 (Sumy: VTD Universytetska knyha, 2005).

³⁰ Герасимов Р.Р. Моделювання при розслідуванні злочинів // Часопис Київського університету права. 2010. № 3. С. 253–256 [Roman R. Gerasimov, *Modeling in the Investigation of Crimes*, 3 Journal of the Kyiv University of Law 253 (2010)].

³¹ Скакун О.Ф. Теорія держави і права: Підручник [Olga F. Skakun, *Theory of State and Law: Study Guide*] 655 (Kharkiv: Konsum, 2006).

³² Полевой Н.С. Криминалистическая кибернетика: теория информационных процессов и систем в криминалистике [Nikolai S. Polevoi, *Forensic Cybernetics: The Theory of Information Processes and Systems in Forensic Science*] (Moscow: Moscow State University, 1982).

2. Results

The e-segment of the pre-trial investigation is one of the most significant in terms of importance, but not fully understood by the criminal process or by the *CPC of Ukraine* in 2012. Providing the bases of the adversarial system in the electronic right-realization environment through the prism of the combination of its normative and technical components is investigated for the first time in this paper.

In accordance with part 2 of Article 22 *CPC of Ukraine*, the parties to the criminal proceedings have equal rights to collect and submit, to the court, files, documents, other evidence, petitions, complaints, as well as the implementation of other procedural rights provided by the *CPC of Ukraine*.

According to para. 63 of the ECHR judgment of 23 June 1993 in the case of *Ruiz-Mateos v. Spain*, the adversarial system means that each party must be given the opportunity to review and respond to all the evidence and observations provided by the other party.³³

One of the innovations of the current *CPC of Ukraine* is the right of the suspect and his/her counsel to familiarize himself/herself with the materials of the pre-trial investigation at any stage (para. 14 of part 3 of Art. 42, part 4 of Art. 46, Arts. 221 and 290 of the *CPC of Ukraine*). The above also includes information from the *Register*. Therefore, at the request of the suspect, the prosecution party is obliged to provide him/her with the information contained in the electronic procedural document. However, the defense is technically not able to directly access the information in the *Register*.

In the opinion of the author of this study, the *URPI* is a structured hierarchical information and analytical database of electronic procedural documents for securing, storing, protecting, recording, searching, compiling and analyzing information about criminal offenses and the persons who committed them, adopted during the process of making procedural decisions, and the procedural actions that were performed (Arts. 103 and 110 of the *CPC of Ukraine*).

Today, the *Register* should be considered as an electronic segment of the pre-trial investigation, which serves as an innovative model for securing a number of procedural decisions and procedural actions. The information provided to the *Register* is processed electronically. According to part 3 of Article 99 of the *CPC of Ukraine*, the original copy of the electronic document is its image, which has the same meaning as the document. Therefore, the *URPI* is an electronic procedural document.

The prosecution party has exclusive authority to have full access to the *Register* as an electronic segment of the criminal process, and to add information and corrections to it. Only the investigator, the head of the pre-trial investigation body, the head of the prosecutor's office, and the prosecutor have direct access to the *Register*.

³³ *Ruiz-Mateos v. Spain*, Application No. 12952/87, Judgment, 23 June 1993, ECHR.

The defense lawyer is in no way involved with the *URPI*, and, therefore, the adversarial system only works in part from the point of view of electronic proceedings. At the same time, the defense party has the undoubted right to receive copies of procedural documents and written communications, as well as to review the materials of the pre-trial investigation in the manner provided for in Article 221 of the *CPC of Ukraine*. Refusal to provide publicly accessible documents, the originals of which are kept in the materials of the pre-trial investigation, is forbidden. However, the reception of the data of the *URPI* by the protection side is not regulated by law. According to part 6 of Article 9 of the *CPC of Ukraine*, when the provisions of the Code do not regulate or ambiguously regulate the criminal proceedings, the general principles of criminal proceedings are applied, as defined in part 1 of Article 7. In this case, the adversarial system provides equal rights of the parties for the exercise of procedural rights of the *CPC of Ukraine*. Consequently, the information from the Register regarding a particular criminal proceeding is a part of the pre-trial investigation material. Therefore, the defense party has the right to get acquainted with and receive copies of the information submitted to the *URPI*.

In accordance with para. 4 of part 1 of Article 24 of the *Law of Ukraine on Advocacy*, the provision of a lawyer with information and copies of documents obtained during the investigation is carried out in accordance with the procedure established by the Criminal Procedure Law.³⁴ In its turn, the *Criminal Procedure Law* (Art. 221) ensures full access for the defense to the materials of criminal proceedings.

According to the *Regulation on the Procedure for Maintaining a Unified Register of Pre-trial Investigations* (hereinafter the *Regulations*), the materials on the application of security measures regarding persons involved in criminal proceedings are not being submitted to the *URPI*.³⁵ With regard to materials that may be prejudiced by a pre-trial investigation, this notion is not legally defined and is more valuable.

After analyzing the list of information submitted to the *URPI*, we believe that a review of the same cannot be detrimental to the pre-trial investigation, since: a) it does not contain information about the amount of evidence collected by the prosecution, or its quality or content; b) it does not contain data that can reveal the plan for conducting a pre-trial investigation, that is, it in no way provides the counsel with information that could be used to counter the investigation. Therefore,

³⁴ Закон України від 5 липня 2012 року № 5076-VI «Про адвокатуру та адвокатську діяльність» [Law of Ukraine No. 5076-VI of 5 July 2012. On Advocacy] (Feb. 12, 2019), available at <http://zakon1.rada.gov.ua/laws/show/5076-17>.

³⁵ Положення «Про порядок ведення Єдиного реєстру досудових розслідувань», погодж. з Міністерством внутрішніх справ України, Службою безпеки України, Державною податковою службою України та затв. наказом Генерального прокурора України від 17.08.2012 р. № 69 [The Regulation “On the Procedure for Maintaining a Unified Register of Pre-trial Investigations,” agreed with the Ministry of Internal Affairs of Ukraine, the Security Service of Ukraine, the State Tax Service of Ukraine and approved by order of the General Prosecutor of Ukraine No. 69 of 17 August 2012] (Feb. 12, 2019), available at http://www.gp.gov.ua/ua/pd.html?_m=publications&_t=rec&id=110522.

the access of a lawyer to criminal proceedings, in which he/she defends a person, is not legally unlimited as regards the information provided to the *URPI* and should be non-alternative, as in the case of access to paper materials. The presented procedural dialogue proves the functioning of the adversarial system in the pre-trial investigation, regardless of the execution format of criminal procedures, meaning that the defense should be allowed to participate in the electronic process.

According to the doctrinal provisions, enshrined in Article 22 of the *CPC of Ukraine* on the principle of equality of parties to the proceedings, subjects of criminal proceedings must be endowed with rights and perform duties corresponding to their procedural status. Consequently, the investigator, prosecutor and lawyer, as special subjects of criminal proceedings, should have the same access to the *Register*. The defense lawyer is endowed with a number of procedural rights, which stipulate the unconditional receipt of information from the *Register*. Therefore, the need for an intermediary between the *Registry* and the lawyer disappears in case of the latter's right to receive information from the *URPI*.³⁶

Bill No. 3262 also supports the above.³⁷ It proposes obliging the prosecutor to submit to the suspect and his/her counsel (and other subjects set out in Article 293 of the *CPC of Ukraine*) a copy of the extract from the *URPI* on the proceedings. The draft bill stipulates that, in the extracts from the *URPI* about the proceedings, the following information should be provided: the date and time of registration of criminal proceedings in the *URPI*; name and surname of the investigator or prosecutor who registered the criminal proceedings; the date, time and the name and surname of the investigator or prosecutor who accepted the criminal proceedings; date, time and the name and surname of the appointed investigator or group of investigators and prosecutor or group of prosecutors; date, time and the name and surname of the investigator or prosecutor who informed the suspect that they were under suspicion; date, time and the name and surname of the investigator or prosecutor who provided the materials of the pre-trial investigation for review by the suspect, his/her counsel, legal representative and the counsel of the person, in respect of which the provision is made for the use of compulsory measures of a medical or educational nature, the completion of pre-trial investigation, and providing access to pre-trial investigation materials; date, time and the name and surname of the prosecutor, who approved the indictment or request for the use of compulsory measures of a medical or educational nature.

The desire of the legislator to at least partially ensure equality of procedural rights of the parties regarding access to information of the electronic segment of criminal

³⁶ Stolitnii 2016, at 349–353.

³⁷ Законопроект № 3262 «Про внесення змін до КПК України щодо Витягу з ЄРДР про рух провадження», ВРУ, 8 жовтня 2015 року [Bill No. 3262 “On Amendments to the CPC of Ukraine regarding the Extraction of the URPI on the Proceedings,” registered in the Verkhovna Rada on 8 October 2015] (Feb. 12, 2019), available at http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=56733.

proceedings deserves a positive assessment. However, this proposal complicates the criminal procedure, requiring additional paper documents.

In the context of the modern information world, the development of the electronic segment of criminal proceedings is being updated. For example, the *DoNotPay* site (<https://donotpay.com>) helps users to challenge unfair parking fines.

A chatbot that provides free legal counsel using AI is now available in all 50 states starting today. This is following its success in New York, Seattle, and the UK, where it was invented by British entrepreneur Joshua Browder. Browder, who calls his invention “the world’s first robot lawyer,” estimates the bot has helped defeat 375,000 parking tickets in a span of two years.³⁸

A New York law firm “hired” the artificial intelligence (AI) ROSS, working on the Watson cognitive computer. Lawyers ask ROSS (<https://rossintelligence.com>) research questions in natural language, just as if they were talking to a human colleague, and the AI “reads” through the law, gathers evidence, draws inferences and returns with a “highly relevant,” evidence-based answer. It also keeps track of developments in the legal system and especially if anything pertains to a lawyer’s specific case.³⁹ Every day we are coming closer to organizing law enforcement with AI as the executor of repetitive legal process algorithms.

Today, the defense party in the criminal process of Ukraine has the right to indirectly access (via the investigator or prosecutor) the *URPI*, which is obviously a temporary phenomenon on the way to becoming a competitive electronic criminal process. The analysis of the electronic segment of the pre-trial investigation shows that the defendant’s procedural status needs to be improved by his involvement in the *URPI*.

The involvement of a defense lawyer in electronic criminal proceedings is differently implemented in the criminal process of other countries.

In Alberta, Canada, in 2009, the Alberta Justice and Solicitor General introduced the “OpenText Content Suite” system for *Enterprise Information Management (ECM)*, designed to manage information flows. Since March 2015, the Content Suite supports a “Criminal e-File,” which provides reception, management and disclosure of information (analogous to the disclosure of materials to the other party, enshrined in Article 290 of the *CPC of Ukraine*), and the exchange of electronic documents between the *Alberta Crown Prosecution Service* courts, police departments, and defense lawyers.⁴⁰

³⁸ Shannon Liao, *World’s First Robot Lawyer’ Now Available in All 50 States*, The Verge, 12 July 2017 (Feb. 12, 2019), available at <https://www.theverge.com/2017/7/12/15960080/chatbot-ai-legal-donotpay-us-uk>.

³⁹ Stacy Liberatore, *Your AI Lawyer Will See You Now: IBM’s Ross Becomes World’s First Artificially Intelligent Attorney*, DailyMail.com, 14 May 2016 (Feb. 12, 2019), available at <http://www.dailymail.co.uk/sciencetech/article-3589795/Your-AI-lawyer-IBM-s-ROSS-world-s-artificially-intelligent-attorney.html>.

⁴⁰ Alberta Justice and Solicitor General: Canadian Provincial Justice System Rehabilitates Criminal Case Management, Sierra Systems (Feb. 12, 2019), available at <https://www.sierrasystems.com/wp-content/uploads/Case-Study-Alberta-Justice-Solicitor-General.pdf>.

Attorneys receive files through the *Disclosure Request Page* of a secured two-factor authentication internet portal (for added security). By clicking on the “Request Disclosure” button, the lawyer starts a workflow inside the electronic system that sorts and edits the case information. Upon completion, the lawyer is notified by email about the disclosure of the information on the case. When the lawyer enters the electronic system and enters the case number, “Disclosure Ready” is shown on the display. A simple one-click interface launches the download feature in the Content Suite, while a copy of the file is stored on the attorney’s computer. Templates (workflow algorithms) that organize information on a case into a standard folder structure in the Content Suite are arranged by business case and include sections for documents, media, and much more. The top-level structure of the folder is its number in the to-do list. Inside each case, 5 standard folders are automatically created, including original documents, working documents, court documents, correspondence, and documents received as part of disclosure by the parties. A sixth media folder is also being created, where photos, videos and any electronic media provided by the police are downloaded.⁴¹ The algorithm for involving an attorney in electronic proceedings and disclosing materials to the other party (Art. 290 of the *CPC of Ukraine*), implemented in the Criminal e-File, should be taken into account when improving the *URPI* and *URLU*.

Electronic criminal proceedings in the Czech Republic are based on the *E-Case Management System*. The electronic document flow between the *E-Case Management System* and other criminal agents, including the defense lawyer, is implemented through the virtual mailboxes, i.e. “data boxes” (Czech. *datových schránek*). On the basis of *Law of the Czech Republic on Electronic Actions and Authorized Conversion of Documents* No. 300/2008 of 1 July 2009 (hereinafter *Law 300/2008*),⁴² the state authorities, local authorities of self-government, natural or legal persons with authority in the field of public administration, lawyers, notaries, liquidators, private prosecutors, legal entities, sole proprietors, etc. are required to create a virtual mailboxes (through an authorized provider with a license) (data boxes) and use them in communication. *Law 300/2008* obliges law enforcement authorities to communicate electronically and equates the service of the document through the data box to “handing over.”

The data box operates using an algorithm under which the law enforcement agency sends a letter (request, call, suspicious notification, other procedural documents, etc.), after the addressee receives and opens it, the system automatically generates a corresponding message to the sender, which is an official document. If the recipient

⁴¹ Canadian Provincial Justice System Rehabilitates Criminal Case Management, OpenText (Feb. 12, 2019), available at https://www.opentext.de/file_source/OpenText/Customers/en_US/PDF/AlbertaJustice-0615-EN2.pdf.

⁴² Zákon o elektronických úkonech a autorizované konverzi dokumentů, 17.07.2008, No. 300/2008 [Law of the Czech Republic No. 300/2008 of 17 July 2008 on Electronic Actions and Authorized Conversion of Documents] (Feb. 12, 2019), available at <http://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=67315&fulltext=&nr=300~2F2008&part=&name=&rpp=15>.

does not open the email within 10 days, the system automatically generates a message about the expiration of the 10-day deadline for review. Under Czech law, such a person is deemed duly notified.⁴³

The legislation of Ukraine as a whole and the *CPC* does not even include an equivalent of the electronic “dialogue” implemented in the Czech Republic between the pre-trial investigation bodies and other actors in the process. The objectively effective format of the described algorithm of communication between the subjects of criminal proceedings in the electronic environment is, in our opinion, extremely relevant to Ukraine.⁴⁴

One of the most striking examples of electronic criminal proceedings is the Swedish criminal justice system, which uses *RIF* (Swedish “*Rättsväsendets Informationsförsörjning*”), a universal system for the exchange of digital information between criminal justice institutions. *RIF* provides a digital exchange of “structured information” and electronic documents (viewed as “unstructured information”) between the segregated electronic systems of the Swedish criminal justice system: *BAS and BUS* (Swedish electronic tax systems), *DurTvå* (Swedish electronic police system), *Cåbra* (Swedish electronic Procurator’s Office – *SPA* and *SECA*), *Vera* (electronic system of the Swedish Judicial Administration, including district courts and appellate courts), etc.

However, the procedure for the opening of criminal proceedings by the defense party in Sweden (in domestic criminal proceedings – Art. 290 of the *CPC of Ukraine*) is not covered by electronic procedures. Therefore, according to the Law, the prosecutor is obliged to provide the defense party with all the materials of the pre-trial investigation in a paper format. However, Swedish prosecutors say that in some cases the defense is provided with such materials in electronic format, recorded on a DVD. There is also an electronic register of lawyers in Sweden, but neither the law nor the procedure for electronic communication and the exchange of procedural documents between the prosecutor and the party in electronic form is implemented in practice.⁴⁵

Therefore, proposals for the involvement of a defense lawyer in electronic criminal proceedings are relevant both for the criminal process in Ukraine and in Sweden, as well as in other states where the processes for the formation of electronic law enforcement procedures in the criminal process are ongoing.

⁴³ Столітній А., Каліна А. Електронне кримінальне провадження у Чеській Республіці // Науковий часопис Національної академії прокуратури України. 2017. № 3. С. 137–146 [Anton Stolitnii & Anastasia Kalina, *Electronic Criminal Proceedings in the Czech Republic*, 3 Scientific Journal of the National Academy of the Public Prosecutor of Ukraine 137 (2017)].

⁴⁴ *Id.* at 143.

⁴⁵ Столітній А., Холмберг Я. Електронне кримінальне провадження Швеції // Вісник прокуратури. 2017. № 6. С. 67–72 [Anton Stolitnii & Jakob Holmberg, *Electronic Criminal Proceedings in Sweden*, 6 Bulletin of the Prosecutor’s Office 67 (2017)].

3. Discussion

The involvement of a lawyer in an electronic criminal proceeding involves, firstly, the legal aspect – the introduction of amendments to the *CPC of Ukraine* and *Regulations* aimed at ensuring regulation of the involvement of a lawyer in the new electronic system, and secondly, the technical aspect: a) improving the technical capabilities of the *Register*; b) integration of *URLU* and *URPI* with the help of an interoperable system for two-way data exchange in real time; c) providing lawyers with electronic digital access keys to the *URPI*.⁴⁶

The legal aspect of the settlement of this issue is the choice of the defense counsel by the user of the *Register*, the creation of a procedure for obtaining an electronic digital key to access it, the consolidation of the procedure for sending electronic procedural documents in the *URPI* between the parties and records such receipt as due and proper by electronic confirmation, consolidation (by the example of the Czech Republic) of a ten-day deadline for the obligation to become familiarized with the electronic procedural documents, after the expiration of which the defense will be considered as properly informed.

The technical aspect involves the creation of a “Defense” subsystem in the *URPI* on the participation of a defense lawyer in proceedings. It will include a set of electronic templates of procedural documents for procedural actions and electronic digital circuits for the adoption of procedural decisions with the help of the *Register*.

In view of the example of the data boxes used in the Czech Republic, it is proposed to create a personal *virtual account* for the lawyers in the *URPI*, i.e. a personal automated workplace of the criminal proceedings which ensures the formation, storage, protection, synthesis, and accumulation of electronic procedural documents, data exchange, strict separation of powers in the system, support of roles depending on the occupied position, and logging and audit of user actions, which will help the person to achieve unimpeded access only to certain *URPI* information relating to his/her competence.

The implementation of a system for lawyer involvement in a particular criminal proceeding is proposed under the following algorithm: the authorized person (body) fills in the electronic template “Engagement of the defense lawyer” in the *URPI*, which is agreed upon by the lawyer indicated in the form (within 24 hours) and, after that, by the investigator or the prosecutor (within 24 hours). The system automatically checks the absence of procedural obstacles for the protection, including the *URLU* system, records such absence and, after the approval, includes the lawyer in the proceedings, giving such lawyer access to the subsystem of the “electronic dialogue.” Access to information on criminal proceedings and electronic procedural documents will be provided to a lawyer on the basis of a decision of the investigator

⁴⁶ Stolitnii 2016, at 355.

and the prosecutor in accordance with Arts. 221 and 290 of the *CPC of Ukraine* and implemented in electronic format: the authorized official enters the data on the transfer of the materials to the *Register* (specifies which files are being transferred, and removes (if necessary) personal data or restricted access information), and after that they appear in the electronic virtual account of the defense.

When the defense is involved by an investigator, prosecutor, or the investigating judge in conducting a separate procedural act (Art. 53 of the *CPC of Ukraine*), the algorithm is as follows: if the suspect is informed of his being under suspicion, the "Protection" subsystem is activated; the lawyer does not visit the investigator, the prosecutor, or the investigating judge twice in order to conduct procedural actions; the System automatically sends an electronic request for the involvement of a lawyer to an authority (institution) authorized by law to provide free legal aid, and also sends a notice of the lawyer's breach of duty to the Qualification-Disciplinary Commission of the Bar. The program then uses the previous algorithm.

After involving a defense lawyer, all entities related to the electronic segment of criminal proceedings are notified through a personal *virtual account*. From now on, the lawyer, with the help of the *electronic digital key (EDK)*, enters the *URPI* and has access to the proceedings in which he/she is identified as a defense lawyer. He/she can now independently generate extracts and involve other participants in the process in the electronic segment.

Therefore, the defense lawyer will be involved in the information system and in the system of "electronic dialogue" between the participants in the criminal proceedings. In order to obtain an extract from the *URPI* or data on the conduct of proceedings, a lawyer can – with the help of an *EDK* – independently do so in a few minutes without leaving his/her workplace. Investigative actions will be imposed by the investigator or the prosecutor in the electronic system, which will automatically inform the lawyer, whose duty will be to ensure the appearance of the defendant. Similarly, it is possible to automate the processing of petitions, the forwarding of documents (regulations), and the opening of pre-trial investigation materials (and so on). In case of a repeated non-appearance of a lawyer without a valid reason, the electronic subsystem of the *URPI*, which must be linked to *URLU*, will automatically be able to send a request for the appointment of a free defense counsel in an order of priority and automatically record this fact in the *URLU* (perhaps also the reason for carrying out the relevant inspection, etc.). Moreover, the lawyer, as a specialized entity, will perform the powers (both from a technical and legal function) of an information intermediary between the *URPI* and the client.⁴⁷

For example, the system of lawyer automatic warning will prevent a violation of para. 1 and item "c" of para. 3 of Article 6 of the *Convention*, as established in the ECHR judgment in the case of *Grinenko v. Ukraine* as the applicant was not entitled to protection under the following factual circumstances:

⁴⁷ Stolitnii 2016, at 355–356.

97. Despite the fact that two defendants were appointed to the applicant, he was repeatedly questioned only in the presence of a lawyer appointed to him by the investigating authorities. There was, however, no evidence that the lawyer invited by the applicant's father was duly informed about such investigative actions.⁴⁸

Granting access to the *URPI* to an attorney creates a potential opportunity for the introduction of automated procedural controls available both to the defense party and to the prosecution party and enforcement in the matter of compliance with the adversarial system rules.

When integrating software algorithms in the *URPI* with the help of ready-made sets of Excel functions, which generate data on violations of criminal procedural legislation, the parties to the criminal process will receive an innovative instrument to ensure the due process of law.⁴⁹ With the help of this system, it is possible to ensure observance of reasonable terms.

This is evident in the light of the judgment of the ECHR in *Vergelsky v. Ukraine*, where the Court noted that, in criminal cases, the "reasonable time" period referred to in para. 1 of Article 6 of the *Convention* begins from the moment of filing an "accusation," i.e. from the moment when the competent authority officially declares that the crime has been committed by someone specific. This definition also meets the criterion for determining when "the (*suspect*) situation has been significantly undermined." With regard to the expiry of the "appropriate period" in criminal proceedings, this period, which is determined by para. 6 of Article 1 of the *Convention*, covers all the time during which the proceedings were conducted, including the time of any appeal against decisions (para. 114).⁵⁰

The application of the *URPI* for the described tasks is precisely effective in light of the entry of information on the notification of the suspect into this electronic system (part 4 of Art. 278 of the *CPC of Ukraine*). According to para. 14 of part 1 of Article 3 means bringing a person to criminal liability, and deducing from this moment the terms of the pre-trial investigation (Art. 219 of the *CPC of Ukraine*), including the automation of this process with the help of an electronic system.

For example, with the help of the *Work No. 57773*, it was discovered that, according to the *URPI*, in 2016 almost 200 offences did not extend the terms of pre-

⁴⁸ *Grinenko v. Ukraine*, Application No. 33627/06, Judgment, 15 February 2012, ECHR.

⁴⁹ Столітній А.В., Аузін Р.О. Аспекти вдосконалення аналітичних та контрольних можливостей Єдиного реєстру досудових розслідувань // Вісник Запорізького національного університету. 2015. № 1. С. 189–199 [Anton V. Stolitnii & Roman O. Auzin, *Aspects of Improving the Analytical and Control Capabilities of the Uniform Register of Pre-Trial Investigations*, 1 Bulletin of the Zaporizhzhya National University 189 (2015)].

⁵⁰ *Vergelsky v. Ukraine*, Application No. 19312/06, Judgment, 12 March 2009, ECHR.

trial investigation by more than 2 months after the suspect was informed of the suspicion (Art. 294 of the *CPC of Ukraine*).⁵¹

Under the condition of implementation in the *URPI* of preventive automated procedural control proposed by the author, the specified data in each separate set of proceedings will be seen by both the investigator and the prosecutor/procedural director as well as the lawyer in the form of alerts on the completion of the specified *CPC of Ukraine* within a certain time period.⁵² This will provide time for subjects not to allow violations. Since this message will be seen by the defense party, this will encourage the party to prosecute the procedure.

In Kyrgyzstan, the involvement of an inquiry agency by an authorized officer, or a lawyer by an investigator or court under legal aid guaranteed by the state is carried out through the state register of lawyers (parts 4 and 5 of Art. 51 of the *CPC of Kyrgyzstan*).⁵³

The electronic procedure for the involvement of a lawyer may be implemented in the criminal process of Ukraine with the help of *URLU*. Ensuring the participation of a defense counsel in criminal proceedings by an investigator, prosecutor or investigating judge in accordance with Article 49 of the *CPC of Ukraine*, or in other cases stipulated by the *Law of Ukraine on Free Legal Aid* of 2 June 2011 (the entities providing such assistance are the relevant centers and lawyers included in the register of lawyers who provide free secondary legal aid on a permanent basis or temporary aid on the basis of a contract) basis and, in general, the introduction of a defense counsel in proceedings involving the presentation of relevant supporting documents by a lawyer is currently fully paper-based.⁵⁴ The corresponding procedure through the interoperable systems between the *URPI*, the electronic court systems, and the *URLU* can be transformed into an electronic format. The obligatory participation of the lawyer in the proceedings is already automated.

⁵¹ Аузін Р.О., Столітній А.В. Твір № 57773: Статистичні дані, отримані за допомогою інформаційно-аналітичної системи обробки заздалегідь згенерованих баз Єдиного реєстру досудових розслідувань за допомогою готових наборів функцій Excel // Державна служба інтелектуальної власності України, 23.12.2014 [Roman O. Auzin & Anton V. Stolitnii, *Work No. 57773: Statistical Data Obtained Through the Information and Analytical System of the Processing of Pre-Generated Databases of the URPI Using the Completed Sets of Excel Functions*, State Intellectual Property Service of Ukraine, 23 December 2014].

⁵² Столітній А.В. Автоматизований кримінальний процесуальний контроль // Вісник Національної академії прокуратури України. 2017. № 3. С. 89–94 [Anton V. Stolitnii, *Automated Criminal Procedural Control*, 3 Bulletin of the National Academy of Public Prosecution of Ukraine 89 (2017)].

⁵³ The Criminal Procedure Code of the Kyrgyz Republic, adopted by the Jogorku Kenesh (Parliament) of the Kyrgyz Republic on 22 December 2016 No. 217 (Feb. 12, 2019), available at <https://www.legislationline.org/ru/documents/section/criminal-codes>.

⁵⁴ Закон України від 2 червня 2011 року № 3460-VI «Про безоплатну правову допомогу» [Law of Ukraine No. 3460-VI of 2 June 2011. On Free Legal Aid] (Feb. 12, 2019), available at <http://zakon2.rada.gov.ua/laws/show/3460-17>.

According to questionnaires, 81.2% of lawyers and 82% of judges (investigating judges) consider it expedient to introduce an automated appointment of a lawyer (free of charge) with the help of the *URPI*, as it is, according to Article 35 of the *CPC of Ukraine*, already implemented in the *Automated System of Document Circulation of the Court* (hereinafter the *ASDCC*) for investigating judges and judges.

It is proposed that the experience of the province of Alberta (Canada) concerning the electronic format for disclosing materials to another party, enshrined in Article 290 of the *CPC of Ukraine* should be applied by way of including the details of the person charged with a criminal offence in the *URPI* to create a secure internet portal with two-factor authentication, which will ensure that a copy of the electronic procedural document is downloaded to the computer for familiarization.

Non-specialized subjects of the criminal process do not need to be involved in electronic criminal procedures using a separate software module or electronic subsystem. If necessary, they can provide explanations, testimonies, and insert their objections into electronic procedural documents. A signature can be made by way of an individual's personal electronic digital signature or by a recently entered ID-passport of a citizen of Ukraine. The executive branch has announced the possibility of using this innovative document to gain access to electronic administrative services. Therefore, with certain improvement of criminal procedures, it can also be used in the sphere of criminal justice for the electronic identification of non-specialized subjects of criminal proceedings.

The described suggestions reflected the concept of electronic criminal proceedings developed by the author, which consist of the formation of criminal proceedings in the form of electronic files and the procedural interaction of the subjects of proceedings in an electronic right-realization environment with the help of high-performing software products with an absolute level of identification.

The author defines the concept of "electronic criminal proceedings" as a criminal procedure based on the compositional algorithms of automated criminal procedures carried out by the subjects in electronic format and recorded in the official electronic procedural document.

It should be noted that the transition of criminal proceedings to an electronic format requires the strengthening of cybersecurity of electronic information systems of the criminal justice authorities. In modern conditions, this is one of the central problems.

The protection of data and software (primarily databases and data warehouses) means a set of activities and appropriate means to protect the property rights of information owners against unauthorized access, use, destruction and any other form of harm. The security threat is treated as a possible danger (potential or actual) of a certain act (action or omission) directed against the object of protection (information resources), which damages the owner or the user and manifests itself in the danger of distortion, disclosure or loss of information. The realization of the

threat is called an attack.⁵⁵ In our opinion, one of the most effective tools to protect against attacks is the cryptographic protection of information. This is a hardware and software system that performs cryptographic information transformation to ensure its confidentiality and integrity. The protection of information can be carried out both in the transmission process through communication channels, and in the process of storing and processing information on the information system's nodes.

In order to improve the quality of cryptographic protection, virtual private networks are used. These are a set of network connections between several means of cryptographic information protection, where information is transmitted in a protected form. Typically, virtual private networks are created on the basis of the communication channels of open data networks, such as the internet.

Within a virtual private network, data can be transmitted in *transport* mode (only the data field is encrypted) or in *tunneling* mode (the data field and the header are encrypted). Creation of a protected tunnel is performed by the virtual network cryptographic protection components that operate on the nodes, between which the tunnel is formed. These components are usually called the initiator and terminator of the tunnel.

The tunnel initiator encapsulates (re-packets) the packets into a new packet containing a new header with information about the sender and the receiver along with the original data. Although all packets sent over the tunnel are IP packets, the encapsulated packets can belong to any type of protocol (for example, NetBEUI).

The tunnel terminator performs a reverse encapsulation process – it deletes the headers and routes each source packet to the local protocol stack or to the destination on the local network. In itself, the encapsulation does not affect the security of message packets transmitted through the tunnel. However, there is a possibility of full cryptographic protection of packets. Confidentiality of such packages is ensured by their cryptographic closure (i.e. encryption), while integrity and authenticity is ensured by the formation of a digital signature.

Since there are a lot of methods for cryptographic protection of data, it is very important that the initiator and terminator of the tunnel use the same methods and can coordinate this information with each other. Furthermore, in order to be able to decrypt the data and verify the digital signature at reception, the initiator and terminator of the tunnel must support secure key exchange functions. It is also important to note that tunnels are created only between authorized users and the end-points of interaction must be authenticated.⁵⁶

Tunneling is used to protect the transmission of *URPI* data via the internet and still confirms its effectiveness. With the complete transition to electronic production, the

⁵⁵ Пархоменко І.І., Квачук О.О., Воскобойніков А.О., Попов Г.В. Тунелювання, як засіб захисту корпоративної інформації // Захист інформації. 2012. № 1. С. 36–39 [Ivan I. Parkhomenko et al., *Tunneling as a Means of Protecting Corporate Information*, 1 Information Protection 36 (2012)].

⁵⁶ *Id.* at 37.

threat of cyber-attack comes almost from every suspect, as well as criminal groups and terrorist organizations. Therefore, such an electronic system must function in a “closed” line, i.e. each computer (another gadget) must be registered in the system to gain access, and the data must be protected by enhanced means of technical and cryptographic information protection.

In order to create conditions for the safe operation of cyberspace, its use in the interests of the individual, society and the state, on 27 January 2016, the National Security and Defense Council of Ukraine approved the *Strategy of Cybersecurity of Ukraine* enacted by Decree of the President of Ukraine No. 96/2016 of 15 March 2016.

Among the methods of ensuring cybersecurity of Ukraine in accordance with the *Strategy*, it is worth mentioning “*Cyber protection of state electronic information resources and information infrastructure intended for information processing, the requirement for protection of which is established by law*” and “*Cyber defense of critical infrastructure*,” which should also include registries and electronic information systems of criminal justice bodies. Therefore, it should be reflected in the *Law of Ukraine on the Fundamentals of National Security of Ukraine*, the *Law of Ukraine on Information Security in Information and Telecommunication Systems*, the *Law of Ukraine on Information*, the *Law of Ukraine on Combating Terrorism*, the *Law of Ukraine on the Basic Principles of Cybersecurity in Ukraine*, the *Criminal Code*, the *CPC of the Ukraine*, and other rules on securing the status of critical information infrastructure facilities.

The cybersecurity strengthening of electronic information systems of the criminal justice authorities need to use the main acts of the European Union on cybersecurity:

- *Council of Europe Convention on Cybercrime (the Budapest Convention)*;⁵⁷
- *Council Conclusions on Improving Criminal Justice in Cyberspace*;⁵⁸
- *Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*;⁵⁹
- *Action Plan for Implementation of the Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*;⁶⁰

⁵⁷ Council of Europe, Convention on Cybercrime, Budapest, 23 November 2001 (Feb. 12, 2019), available at http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest/_7_conv_budapest_en.pdf.

⁵⁸ Council of the EU, Council Conclusions on Improving Criminal Justice in Cyberspace, Luxembourg, 9 June 2016 (Feb. 12, 2019), available at <http://www.consilium.europa.eu/media/24300/cyberspace-en.pdf>.

⁵⁹ Council of the EU, Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, Brussels, 20 November 2017 (Feb. 12, 2019), available at <http://www.consilium.europa.eu/media/31666/st14435en17.pdf>.

⁶⁰ Council of the EU, Action Plan for Implementation of the Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, Brussels, 12 December 2017 (Feb. 12, 2019), available at <http://data.consilium.europa.eu/doc/document/ST-15748-2017-INIT/en/pdf>.

- *Legislative Proposal on Access to Electronic Evidence in Criminal Investigations*;⁶¹
- *Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*;⁶²
- *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*;⁶³
- *European Parliament Resolution of 3 October 2017 on the Fight Against Cybercrime*.⁶⁴

All the above documents are important for creating effective protection of information systems. As part of our research, we consider it appropriate to analyze the following documents.

The *Budapest Convention* defines the application of this Convention by Parties in para. “c” of part 2 of Article 14, including Ukraine, of the powers and procedures for the collection of evidence in electronic form in respect of a criminal offence. The Convention corresponds to the provisions of para. 2 of part 1 of Article 103 of the *CPC of Ukraine* concerning the storage of procedural actions on the information carrier during criminal proceedings with the help of technical means; as well as Article 99 of the *CPC of Ukraine* on the documented definition for materials of photography, sound recording, video recording, and other media (including electronic) and the settlement of the procedural status of an electronic document. This allows the parties to the criminal process of Ukraine to collect evidence in electronic form and apply it in procedural activities, which enhances the effectiveness of criminal proceedings. However, today there are no effective procedures for electronic interaction between the parties to criminal proceedings, particularly with regard to the exchange of evidence recorded in electronic form. Therefore, the suggestions we have made regarding the involvement of the defense in the information field of the *URPI* and the system of “electronic dialogue” between the parties to the criminal proceedings take into account and develop the provisions of the convention on the collection of evidence in electronic form.

The importance of ensuring effective electronic interaction between the parties to the criminal process in Ukraine, particularly regarding the receipt of electronic

⁶¹ Legislative Proposal on Access to Electronic Evidence in Criminal Investigations, Inception Impact Assessment, 3 August 2017 (Feb. 12, 2019), available at <https://publications.europa.eu/en/publication-detail/-/publication/b2f853ff-7868-11e7-b2f2-01aa75ed71a1/language-en>.

⁶² Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, JOIN/2017/0450, Brussels, 13 September 2017 (Feb. 12, 2019), available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN>.

⁶³ Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, COM/2018/225, Strasbourg, 17 April 2018 (Feb. 12, 2019), available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN>.

⁶⁴ European Parliament Resolution of 3 October 2017 on the Fight Against Cybercrime, 2017/2068(INI) (Feb. 12, 2019), available at <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2017-0366>.

evidence in criminal justice, is the *Council Conclusions on Improving Criminal Justice in Cyberspace*.⁶⁵ We agree with the scope of the recommendations to increase cooperation with service providers for the rapid disclosure of data; mutual legal assistance procedures for accelerating and simplifying the circulation of electronic data; and effective use of mutual recognition procedures for the effective provision and receipt of electronic evidence. The properties of electronic criminal proceedings suggested in this article allow the following proposals to be implemented: the use of standardized forms and tools in order to simplify authentication, provision of fast procedures and increased transparency and responsibility for providing and obtaining electronic evidence; obtaining electronic evidence; adapting standardized forms and procedures for providing and obtaining electronic evidence (for example, their creation in electronic format); increasing the effectiveness of using such standardized forms and procedures with the help of existing electronic tools (for example, their exchange with the help of the *URPI*); and collaboration on direct cross-border access to data without technical assistance (for example, the implementation of such access with the involvement of the *URPI*).

The *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*⁶⁶ aims to improve legal certainty for authorities, service providers and persons affected and to maintain a high standard for law enforcement requests, thereby ensuring the protection of fundamental rights, transparency and accountability. It is valuable for the criminal process in Ukraine and we consider it necessary to apply a number of its provisions during the implementation of electronic criminal proceedings in Ukraine. As regards the European Production Order, the European Preservation Order and Certificates, in our opinion, the appropriate electronic criminal procedures in the order of electronic criminal proceedings should be realized on the basis of the *URPI*.

Conclusion

In the context of the modern electronic-legal criminal process of Ukraine, which is currently undergoing a transitional stage between paper and purely electronic, the adversarial system has gained new content for the parties to the criminal proceedings. In order to improve it, we see the need to reform the criminal (electronic) process of Ukraine by bringing the defense party to the *URPI*.

The author carried out a practical experiment in the form of theoretical modelling and practical implementation of the algorithm for the implementation of electronic criminal procedures. During this experiment, which was based on a sample of twenty five criminal proceedings, the practice of processing procedural documents was

⁶⁵ Council of the EU, Council Conclusions on Improving Criminal Justice in Cyberspace, *supra* note 58.

⁶⁶ Proposal for a Regulation of the European Parliament, *supra* note 63.

carried out in electronic format, storing procedural actions with the help of technical means, communication of the parties to the proceedings with the help of modern information telecommunication technologies and sending documents by email, provision of pre-trial investigation materials in order of discovery in electronic format. The described experiment demonstrated the high efficiency of tried and tested electronic criminal procedures in terms of reducing time resources on the procedural design of criminal proceedings, high detailing of the course and results of investigative (search) actions and secret investigative (search) actions, as well as simplifying the procedure for opening pre-trial investigation materials with the provision of electronic materials in the form of shortcuts of the timing of this procedure with simultaneous, not time-limited, study of the corresponding electronic mappings.

The participation of a lawyer in electronic criminal proceedings involves improving the technical capabilities of the *URPI*, its integration with the *URLU*, and providing lawyers with electronic digital keys to access the *URPI*. In legal terms, the process of sending electronic procedural documents in the *URPI* between the parties is enshrined in the procedural law. The access of the lawyer to the information in the Register is ensured by creating a personal virtual (electronic) office. With regard to categories of proceedings in which the participation of a lawyer is mandatory, it is proposed to automate the process of his/her involvement in a specific criminal proceeding with the help of the *URLU*.

The proposed automatic involvement of the lawyer is also relevant in case of the need to ensure the right to protection in criminal proceedings at its initial stage. The legal position of the ECHR is set forth in para. 63 of the ECHR judgment of 9 June 2011 in the case of *Luchaninova v. Ukraine*, which states that “in order to carry out the defendant’s right to protection, he should normally be provided with the effective assistance of the counsel from the very beginning of the proceedings” (para. 52 of the ECHR judgment of 27 November 2008 in the case of *Salduz v. Turkey* and paras. 90–91 of the ECHR judgment of 12 June 2008 in the case of *Yaremenko v. Ukraine*).⁶⁷

The integration of electronic systems and specialized criminal entities through interoperability systems by way of involvement of specialized entities and the provision of a permanent user’s digital signature will enable the creation of an effective professional procedural “electronic dialogue” and provide permanent remote access to investigation materials, and the creation of personal “virtual accounts.” It will also ensure the organization of a special mode of access to electronic procedural documents, taking into account the procedural position of the subject occupying his/her position or scope of powers (differentiation of access levels) and their protection against unauthorized editing, removal or concealment. As a result,

⁶⁷ See *Luchaninova v. Ukraine*, Application No. 16347/02, Judgment, 9 June 2011, ECHR; *Salduz v. Turkey*, Application No. 36391/02, Judgment, 27 November 2008, ECHR; *Yaremenko v. Ukraine*, Application No. 32092/02, Judgment, 12 June 2008, ECHR.

the subject of the proceedings will only have access to those proceedings, in which this particular person participates and only to the extent necessary for procedural actions or the adoption of procedural decisions.

While working on this article, the object of research in the form of an electronic segment of criminal proceedings was analyzed using software products such as *URPI*, *URLU*. The information-analytical system of the processing of pre-generated databases of the *URPI* using the ready-made sets of Excel functions was used by the author. By processing the pre-formed and stored databases, the *URPI* generates data for more than 30 types of violations of criminal procedural law and is an element of electronic procedural control.⁶⁸

The concept of electronic criminal proceedings is the formation of criminal proceedings in the form of an electronic file and the procedural interaction of the subjects of proceedings in the electronic right-realization environment with the help of high-performance software products with an absolute level of identification. An integral part of the proposed electronic format of criminal procedural activity is the implementation of electronic criminal procedures in conditions of providing a high degree of technical and cryptographic protection of information.

The obtained results of the research can be further used to improve the criminal procedural activity in Ukraine in the form of the legal and technical algorithms for involving the protection party in the electronic law enforcement environment of the criminal process. This study is also relevant to the practice of the criminal process in the states that are actively using electronic criminal procedures, since it offers a way to address specific problematic issues. For example, the electronic criminal process in the Czech Republic is characterized by a high level of development of electronic criminal proceedings though the adversarial system is implemented in the form of paper procedural documents.

However, the described idea needs to be developed, because the proposed model of electronic dialogue is only the first step in reform of the electronic segment of the criminal process, which will modernize the bureaucratic, multi-stage and intricate system of paper dialogue. It will become a prerequisite for the introduction of "electronic criminal proceedings."

References

Epps D. *Adversarial Asymmetry in the Criminal Process*, 4(91) New York University Law Review 762 (2016).

Findley K.A. *Adversarial Inquisitions: Rethinking the Search for Truth*, 56 New York Law School Law Review 911 (2011).

⁶⁸ Stolitnii & Auzin 2015, at 189–199.

Kirchengast T. *Victim Lawyers, Victim Advocates, and the Adversarial Criminal Trial*, 16(4) *New Criminal Law Review* 568 (2013).

Langbein J.H. *The Origins of Adversary Criminal Trial* (Oxford: Oxford University Press, 2003).

MeUlli K.J. *Prosecutorial Discretion in an Adversary System*, 1992(3) *BYU Law Review* 669 (1992).

Ogg J.T. *Adversary and Adversity: Converging Adversarial and Inquisitorial Systems of Justice – a Case Study of the Italian Criminal Trial Reforms*, 37(1) *International Journal of Comparative and Applied Criminal Justice* 31 (2013).

Information about the author

Anton Stolitnii (Zaporizhia, Ukraine) – Associate Professor, Department of Criminal Procedure and Criminalistics, Classical Private University (70B Zhukovskogo St., Zaporizhia, 69002, Ukraine; e-mail: stoleta16@gmail.com).