ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.39 Nº 71
2021

Cuestiones Políticas Vol. 39, Nº 71 (2021), 317-333
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Problems of implementing international digitalisation standards of criminal investigation

DOI: https://doi.org/10.46398/cuestpol.3971.16

Valerii I. Bozhyk *
Yan V. Streliuk **
Vitaliy A. Maziychuk ***
Anatoliy O. Voightko ****
Myroslava V. Kokoshko *****
Anatoliy M. Kisliy ******

Abstract

The study consisted of identifying the existing problems in the implementation of international standards of digitization of criminal investigation at the legislative level. The research was carried out in stages as a summary, based on the logic of presentation of the material, to achieve and meet the objectives set out in the article. The method of direct observation, the method of comparison and analysis of the content of the documents, the method of systemic and pragmatic approach were used. The key results of the study were the analysis of the experience of implementing digital standards in forensic activities in the United States, Canada, Great Britain, Denmark, England, Austria, Estonia, and Ukraine. It is concluded that the problems that exist in the implementation of these standards, were identified from the criteria of evaluation of the efficiency and capacity of digital data processing by the agencies involved in the criminal investigation. In addition, the problems and

* PhD in Law, People's Deputy of Ukraine, The Verkhovna Rada of Ukraine, 01008 Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0003-3162-0125

** Doctor in Law, Professor, Anti-Corruption and Law Enforcement Department, Educational and Scientific Institute of Law, Prince Vladimir the Great Interregional Academy of Personnel Management, 03039, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-4209-2017

*** PhD in Law, Associate Professor, Anti-Corruption and Law Enforcement Department, Educational and Scientific Institute of Law, Prince Vladimir the Great Interregional Academy of Personnel Management, 03039, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-5309-4413

**** PhD in Law, Associate Professor, Anti-Corruption and Law Enforcement Department, Educational and Scientific Institute of Law, Prince Vladimir the Great Interregional Academy of Personnel Management, 03039, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-4204-7662

***** PhD in Law, Associate Professor, Department of Service and Medical Law, Institute of Law, Taras Shevchenko national University of Kyiv, 01033 Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-5753-9061

****** Doctor in Law, Director, Educational and Scientific Institute of Law, Prince Vladimir the Great Interregional Academy of Personnel Management, 03039, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-4152-9539

Recibido el 15/10/2021 Aceptado el 11/11/2021

difficulties faced by the authorities in implementing existing international digitization standards, indicate the need for comprehensive measures to organize criminal investigations. To overcome them, appropriate measures must be taken in the field of legislative changes.

Keywords: data digitization; criminal investigation; police; international standards; implementation of legislative changes.

Problemas de implementación de los estándares internacionales de digitalización de la investigación criminal

Resumen

El estudio consistió en identificar los problemas existentes en la implementación de los estándares internacionales de digitalización de la investigación criminal a nivel legislativo. La investigación se llevó a cabo por etapas a modo de resumen, basándose en la lógica de presentación del material, con el fin de lograr y cumplir los objetivos planteados en el artículo. Se utilizó el método de observación directa, el método de comparación y análisis del contenido de los documentos, el método de enfoque sistémico y pragmático. Los resultados clave del estudio fueron el análisis de la experiencia de implementación de estándares digitales en actividades forenses en Estados Unidos, Canadá, Gran Bretaña, Dinamarca, Inglaterra, Austria, Estonia y Ucrania. Se concluye que los problemas que existen en la implementación de estos estándares fueron identificados a partir de los criterios de evaluación de la eficiencia y capacidad de procesamiento de datos digitales por parte de los organismos involucrados en la investigación criminal. Además, los problemas y dificultades que enfrentan las autoridades en la implementación de los estándares internacionales de digitalización existentes indican la necesidad de medidas integrales para organizar la investigación criminal. Para superarlos, se deben tomar las medidas adecuadas en el campo de los cambios legislativos.

Palabras clave: digitalización de datos; investigación criminal; policía; estándares internacionales; implementación de cambios legislativos.

Introduction

The development of scientific and technological progress entails changes in the economy, society and politics. In this context, the methods and technology of investigation and detection of crime have changed towards digitalisation of criminal investigation (Janaki, 2019). The technological impulse completely penetrated into the process of data collection in the course of criminal investigation (Alrwishdi, 2021). The outdated written hard copy forms of interaction in criminal investigations turned out to overload the law enforcement system and make it ineffective (Churikova *et al*., 2021). The main task of digital technology is to form evidence by searching, recording and investigating various objects related to criminal proceedings (Antonov *et al*., 2019).

Besides, the location and time of a criminal offense can be found and sometimes predicted quickly thanks to digital technology. The task of fighting crime and protecting citizens becomes almost impossible without the use of digital technology. In turn, citizens and criminals are adapting to the world of digital data faster than police officers (Deloitte, 2015). This requires that bodies involved in criminal investigation to comply with international digitalisation standards.

All possible technologies needed to digitise criminal proceedings have already been developed and are widely available for implementation (Ishchenko, 2019). Therefore, it can be unequivocally stated that the system of criminal prosecution receives great benefits from the implementation of digital technology standards in its procedural activities.

The digital form of recording the criminal investigation is an inevitable future that will simplify the process of storing and retrieving criminal case materials in archives (database files) and improve the quality of the investigator's work. At the same time (Artamonova *et al*., 2021), law enforcement agencies acknowledged the lack of general interest in the digitalisation of criminal investigation, as this could lead to further reductions in staff or equipment needed in their activities. However, early digitalisation was the reason why it was difficult for prosecutors to interpret electronic evidence (Goodison *et al*., 2015).

Information and communication technologies are constantly evolving, so in order to detect cybercrime, the employees involved in criminal investigation must be "life-ling students". In such circumstances, police officers must be constantly trained to stay abreast of the latest technology, to study cybercriminals, their motives, tactics and methods of work. In turn, national security forces experience a so-called "brain drain", when highly qualified and experienced cybercrime investigators leave these agencies to work in private firms, with higher salaries for their knowledge and skills (Harkin *et al*., 2018).

Thus, the issue of implementing digitalisation standards in criminal investigation is relevant both in the world and at the national level.

1. Literature review

Given the fact that the criminal investigation is aimed at obtaining primary information regarding criminal proceedings, the inquest can be built on the basis of the information obtained. Therefore, the main problem that arises during the implementation of digitalisation standards is to determine the limit and scope of the type of digital information that can be provided to a person against whom criminal prosecution is conducted. In this context, the information balance of the interests of the investigation and the public should also be ensured. In turn, the transparency of the criminal investigation for society should not interfere with effective and simple interaction between law enforcement agencies and coordination of their activities, etc.

The use of computer simulator programmes in the course of criminal investigation is not entirely justified. The computer programmes that simulate the process of committing a crime do not exclude the possibility of falsification of evidence, as there are no clear criteria for such programmes, there is enough data collected in different criminal situations (Przhilenskiy, 2020).

A clearer understanding of organizational barriers and professional challenges, as well as a more detailed picture of how electronic evidence can assist police in investigations, is needed to substantiate allegations more empirically about how digitalisation contributes to changing the principles of criminal investigation (Wilson-Kovacs, 2021).

The effectiveness of the use of data from digital networks depends on many factors, and the method of obtaining intelligence information can have both positive and negative results. First, the digitalisation of criminal investigation requires a police officer to have a number of skills and abilities, namely:

- effectively and objectively use search engines and other opportunities to obtain electronic data.
- correctly arrange and analyse the information obtained and draw appropriate conclusions that are important for operative action.
- follow the procedure of correct recording and capture of the data obtained in accordance with the regulatory documents and procedural legislation, which regulate the admissibility of evidence in criminal proceedings.

Besides, it has been found that attempts to optimize the flow of documents in connection with the transition to a new method of electronic data processing leads to an increased flow of such data. At the same time, the volume of the created database increases, which, in turn, requires even more skills and abilities of the user in terms of their rational analysis and interpretation. The information itself, and especially large databases, without proper analysis and processing are insignificant (Tambovtsev and Pavlichenko, 2021) Law enforcement agencies receive a large amount of information and must be able and willing to analyse it in an automated way (Fatih and Bekir, 2015).

The aim of this study was to establish the problems that exist in the implementation of the main international digitalisation standards of criminal investigation at the national level.

The aim provided for the following objectives: identify criteria for assessing the ability to use digital data by the bodies involved in criminal investigation; determine the range of digitalisation standards of criminal investigation that are applied in the world and at the national level; find out the experience and problems faced in the world and at the national level during the implementation of the digitalisation standards of criminal investigation.

2. Methods

The study was conducted through the following methods: direct observation was used to establish the opinion of modern scientists and researchers in the field of digital technology in forensics and clarified the experience of implementing digital standards in forensics, USA, Canada, UK, Denmark, England, Austria, Estonia and Ukraine; the analysis of the content of documents helped identify the main international forensic digitalization standards developed by the International Organization for Standardization and the International Electrotechnical Commission, as well as the criteria for evaluating the effectiveness and capability to process digital data by the bodies involved in criminal investigation; the method of comparison was used to compare the criteria for assessing the effectiveness and ability to process digital data by bodies involved in criminal investigation with international digitalization standards of criminal investigation, resulting in the identification of problems faced by national government agencies in the implementation of existing international digitalization standards; recommendations and proposals for overcoming problems of the implementation of international digitalization standards of criminal investigation at the national level were developed through a systemic and pragmatic approach.

The main tool for obtaining information on the research topic were the views and position of scientists on the introduction of digitalization standards in the criminal investigation activities of police. It was established that the main purpose of these standards is to promote advanced methods and processes of finding and preserving the authenticity of digital evidence, to be able to compare and contrast with each other. Examining separately the training standards that are currently used to train specialists in operational police units, it was found that they do not provide at the national level in-depth knowledge of the methods of obtaining information. Examining the standards for the search and analysis of electronic evidence by the bodies involved in criminal investigation, it was proved that digital information should be obtained without abusing interference in a person's private life. At the same time, digital evidence is often collected incorrectly and analyzed inefficiently, or simply not noticed due to technical difficulties, and therefore the obtained digital data should be studied by specialists who know how to work effectively, analytically, comprehensively, and fairly with large databases.

Separately considering other concepts of forensic activity, it was found that despite the existence of the mechanisms and standards for digitalization, many information technologies have not been properly enshrined in law.

A total of 40 sources and references were used in the work.

3. Results

Mobile computers were the most used technology in policing and tested in police examinations. A study of a separate U.S. police department that implemented a special wireless mobile broadband access system found that its implementation contributed to saving working hours and performing special tasks more efficiently (Carter and Grommon, 2015). A study by the UK government showed that the use of artificial intelligence in the digital police system can have real benefits not only in the fight against crime, but also for the public.

A study conducted among officers in Ontario, Canada, showed that information transmitted informally (through informal social networks) is and will be more relevant, detailed, reliable and secure. The ability of social networks to provide intelligence information can be more useful in criminal investigation only to understand the information dissemination trends (Sinclair Cotter, 2015).

A study in Denmark, England, Austria, and Estonia found that digitalization should be primarily part of the ongoing or long-term process of improving investigative activities of the police. In this context, the

best approach depends on the specific country and the goals underlying digitalization. It should be noted that digitalization is not the goal, it is a tool to promote rationalization and increase the efficiency of crime investigation (De Blok *et al*., 2014).

The study conducted among Norwegian police officers is worth mentioning. It is established that the digitalization of policing leads to a broader division of labor: new positions, new specialties appear, the method of managing police officers changes within the institution (department) towards bureaucratization. That is, the control of policing at a distance, the use of new technologies and standards for stronger management can be considered as a transition to a new form of digital leadership (Gundhus *et al*., 2021).

A study of law enforcement activities of police in Russia found that there is a tendency to complicate the procedure for obtaining electronic data. It was also clarified that the use of computer data should take place only in the manner prescribed by procedural law. Therefore, the investigator must be able to use them properly during the investigation (Stelmakh *et al*., 2021).

The training standards currently used to train specialists to work in operational police units do not provide in-depth knowledge of the methods of obtaining information necessary for the detection and investigation of crimes in the modern information environment and the development of relevant skills. Most employees involved in criminal investigation do not have the appropriate analytical skills and skills to work with large databases.

It has become necessary for the digitalization of criminal investigation procedures to be consistent and to ensure harmony between lawyers, judges, forensic experts, law enforcement agencies, corporations, and individuals. International digital forensic standards and procedures aim to improve the effectiveness of investigations, ensure the admissibility and accuracy of digital evidence and include identification, collection, acquisition and storage. At the same time, standards for storage, ensuring accuracy, completeness and persuasiveness of digital evidence are extremely important, as they are used at the stage of criminal proceedings (Yeboah-Ofori and Brown, 2020)

So, let's cover the main international forensic standards for digitalization that should be used during the criminal investigation (Table 1). These standards were developed by the International Organization for Standardization (hereinafter — ISO) and the International Electrotechnical Commission (hereinafter — IEC).

Table 1. The main international forensic standards for digitalization, which should be used during the criminal investigation (author's development)

ISO/IEC 27043:2015	A general standard that provides guidance on how to reproduce a criminal incident preparation procedure, in the form of idealized models for different scenarios, so that such reproduction can be repeated in each scenario and produce the same result. It includes processes from preparation for the incident to closing the investigation, as well as any general advice on such processes. The provisions of the standard describe the processes and principles applicable to various types of investigations. Unauthorized access, damage to digital data, technical malfunctions of the information system or corporate violations of information security and other digital investigations (ISO, 2015a).
ISO/IEC 27037:2012	A standard that contains guidelines for processing digital evidence, which includes identifying, collecting, obtaining, and storing potential evidence. It assists organizations in their disciplinary proceedings, and also facilitates the exchange of potential digital evidence between jurisdictions (ISO, 2012).
ISO/IEC 27041:2015	The standard, which guarantees the handling of criminal incidents, specifies the procedure for processing evidence, storage and methods used in the investigation process. The purpose of the standard is to provide guidance on: the collection and analysis of data on information security incidents investigation; use of validation of investigation processes; assessment of the level of validation of evidence, and the volume of data required for the audit (ISO, 2015b).
ISO/IEC 27042:2015	A standard that provides guidance on what tools, techniques, and methods to use in analysis and interpretation to ensure continuity, reliability, reproducibility, and repeatability. It includes best practices in the selection, development and implementation of analytical processes and registration of the information obtained, which allows, if necessary, to subject such processes to independent verification (ISO, 2015c).
ISO/IEC 27050-1:2019	The standard provides a definition of electronic discovery (hereinafter — ESI). Besides, it defines related terms and describes concepts, including, but not limited to, identifying, storing, collecting, processing, reviewing, analysing, and creating ESIs. This document also defines other relevant standards (e.g., ISO/IEC 27037) and how they relate to and interact with electronic device detection activities (ISO, 2019).

Besides, we outline the criteria for assessing the effectiveness and ability to process (collect and process) digital data by the bodies involved in criminal investigation (Table 2).

Table 2. Criteria for evaluating the effectiveness and ability to process (collect and process) digital data by bodies involved in criminal investigation (author's development)

Availability of appropriate software and hardware	Changes made to the organizational and procedural documents on the activities of the bodies involved in criminal investigation	Responsibilities of institutions, enterprises, organizations and individuals to assist with the bodies involved in criminal investigation	Prerequisites and guarantees for the preservation of digital data that can be provided to the bodies involved in criminal investigation	Opportunities for the exchange of digital personal data at the request of the bodies involved in criminal investigation	Availability of staff in the bodies involved in criminal investigation, who are able to work rationally with large databases
Are there appropriate electronic devices, computers and analytical software for search and analysis?	Compliance with the regulatory approach to digitalization and departure from previous methods of work of the bodies involved in criminal investigation	Provision of the coordination of activity of bodies involved in criminal investigation on search and requesting of data is provided, and in persons who give them — the relevant duty	Is there relevant information infrastructure and whether cybersecurity bodies operate at the state level	There are technical means and legal opportunities for the accumulation and requesting of electronic data	Working with large databases requires analytical and effective user skills

At the legislative national level, criminal investigation is aimed at finding and confirming data on illegal actions of persons or groups of persons for which criminal liability is provided. Criminal investigation also aims to stop the intelligence and subversive activities of special services of foreign states and organizations, and to obtain information in the interests of the security of citizens, society and the state. In order to exercise their powers, the bodies involved in criminal investigation are already vested with many rights related to the processing of digital data. They can carry out audio and video surveillance of a person, obtain information from transport telecommunication networks, electronic information networks, collect information about the illegal activities of persons subject to inspection; use and create automated information systems, etc. (Verkhovna Rada of Ukraine, 2020).

In turn, the national telecommunications operators are obliged to implement the technical means on the telecommunications networks on their own necessary for the criminal investigation to be carried out by the authorized bodies and to prevent leakage of information about them (Verkhovna Rada of Ukraine, 2004). Besides, personal data may be provided to law enforcement agencies in the interests of national security and human rights (Verkhovna Rada of Ukraine, 2010). Thus, criminal procedure law gives the relevant authorities the right to receive restricted information to perform their functions. That is, the legislative regulation of the rights of the bodies involved in criminal investigation partially testifies to its legal probative force, as a preliminary investigative act provided by the criminal procedure legislation (Verkhovna Rada of Ukraine, 2013).

However, funding, as well as the provision of material and human resources for criminal investigation remains insufficient. The European Union is helping Ukraine in many ways to strengthen its capacity to fight organized crime. To support the e-learning platform of the academies of the Ministry of Internal Affairs in 2020, Ukraine received server stations in almost all regional centers. Such servers are part of a technical upgrade aimed at improving policing efficiency. Two modular data processing centers have also been established in Ukraine with the EU's assistance to increase the secure and timely exchange of data between regional authorities and the national police. The EU and UNOPS have supplied about 200 computers to the Ministry of Internal Affairs (EUAM Ukraine, 2020). Besides, Ukraine received modern servers and data storage systems in 2021to create an IT system to coordinate the work of the national police with Interpol (Europol) in the fight against organized crime (United Nations, 2021).

The fight against cybercrime provides for the involvement of relevant teaching staff in the national police training system to perform the following tasks:

- improvement of procedural mechanisms for collecting electronic evidence.
- appropriate training and preparation of investigators to work with electronic evidence (Ismaylov, 2017).

Improving social control efforts to reduce crime is also relevant at the national level. The expansion of information technology, big data and related approaches is expected to become critical. To this end, law enforcement could in turn teach the community how to use new technologies to prevent crime. It is necessary to establish interaction with the community and increase the effectiveness of crime prevention by providing Internet access in different parts of the country (Stubbs-Richardson *et al.*, 2018).

Given the above, we group the typical problems faced by national authorities in the implementation of existing international digitalization standards of criminal investigation (Table 3).

Table 3. Typical problems faced by national authorities in the implementation of existing international digitalization standards of criminal investigation (author's development)

Insufficient level of training and education of investigators to work with information obtained during the criminal investigation to ensure its compliance with admissibility and relevance	Inadequate level of training specialists who are able to work in a large information environment, with large databases	Inadequate level of cooperation between the police and the community in the field of crime prevention	Insufficiently regulated criminal investigation in terms of recording, exchange, and application of electronic evidence	Inadequate level of material and financial support of bodies involved in criminal investigation

4. Discussion

Digital technologies create problems in terms of equality for all citizens. Detention procedures using modern technology are more likely to be used against minority and foreigners. Another example of using the software to identify and search for faces is recognizing faces in public places. Such technical errors can lead to mistakes in court and illegal acts. With regard to privacy, digital technologies also have some gaps. Privacy is a fundamental human right. But in the digital environment, large amounts of personal data are accumulated against people without proper permission, which can be used against us. We constantly provide data about our location, political views, family life, and we do not know who will use this data, how and why. Therefore, sufficient attention must be paid to the risks posed by digital technologies (Mijatović, 2019). Personal data from mobile phones should be removed with minimal interference with privacy.

To use information in electronic form as evidence in accordance with accepted standards, its entire life cycle shall be subject to procedural enshrinement. It should be provided for identification, research, copying, attachment of the materials to the case and direct use as evidence at the legislative level. To do this, it is necessary to change the conceptual and regulatory approaches to the methods of collecting, studying, belonging and admissibility of digital evidence used in criminal proceedings, at the national level.

The ISO 27037 standard adopted in 2012 will increase awareness of the specifics of working with digital traces and evidence. However, the first part of it can be considered as a mandatory basis in the development and implementation of procedures for the collection of digital evidence. Aa the same time, the second part of this standard, which already contains certain procedures, is now obsolete.

The main goal of the ISO 27k group of digital forensic examination standards are to promote advanced methods and processes of searching for digital evidence. While individual investigators, organizations, and jurisdictions may well maintain their methods and controls in accordance with local laws and established practices, it is hoped that standardization will lead to adoption of similar approaches to criminal investigation at the international level, making it easier to compare, combine, and contrast the results of such investigations (ISO, 2018).

Many terms or concepts of information technology have not yet been legally enshrined. Recognition and standardization of terminology in the legal context of forensic activities are extremely important to prevent miscommunication by law enforcement agencies. Digital evidence is often collected incorrectly and analyzed inefficiently or simply overlooked due to technical difficulties. Specific legal rules and principles should be followed in order to fulfil the tasks of the investigation and to ensure fairness in the conclusions (Nortje and Myburgh, 2019).

The system for recording and collecting digital data in Ukraine should be oriented at potential victims of crime, be transparent to the public, inclusive, and comply with international norms and standards (Council of Europe, 2020).

The above criteria for assessing the ability to use digital data by the bodies involved in criminal investigation indicate the degree of the country's readiness to implement digitalization standards. At the same time, the training and education of highly qualified staff for the system of bodies involved in criminal investigation requires time and adaptation of training programs to perform analytical work.

Conclusion

The experience of the United States, the United Kingdom, and Canada has shown significant benefits from the digitalization of policing. However, the experience of digitalization in Denmark, England, Austria, and Estonia has shown that digitalization is not the goal, it is a tool to promote rationalization and increase the efficiency of criminal investigation.

The use of digital data in the criminal investigation should take place exclusively in the manner prescribed by procedural law, in compliance with international standards. The main purpose of international standards is to promote advanced methods and processes for finding and preserving the authenticity of digital evidence, to compare them.

In the age of digital technology and large amounts of data, crime prevention places new demands on the work of employees involved in

criminal investigation who are able to work with databases. However, national employees are lacking, or their level of training is insufficient. Little attention is also paid to the protection of objects used for electronic communication and exchange of information with pre-trial authorities. It will be appropriate to involve the public in interaction and cooperation as regards crime prevention. However, work in this direction is slow.

Thus, the typical problems faced by national government agencies in the implementation of existing international digitalization standards indicate the need for comprehensive measures to organize criminal investigation. Appropriate steps should be taken in both the legislative and material areas. Besides, the training system of the police officers should involve highly qualified teaching staff, and the digitalization of policing itself should not bureaucratize criminal investigations. The transition to a digital form of law enforcement should take place in parallel: at the level of the bodies involved in criminal investigation, and at the level of investigative bodies and prosecutors.

The conclusions and recommendations given in this study can be used in rule-making and practical activities, in the training of police officers and investigators on the digitalization of criminal investigation. Prospects for further research include paying attention to the problems of digitalization of the activities of investigative bodies in the legislation of Ukraine.

Bibliographic References

ALRWISHDI, Deyaa. 2021. Reconsidering the Digitalization of International Criminal Justice. Available online. In: https://www.justsecurity.org/74166/reconsidering-the-digitalization-of-international-criminal-justice/. Consultation date: 16/04/2021.

ANTONOV, Igor; RAKHMATULLIN, Ramil; BURGANOVA, Guzel; MAKOLKIN, Nikita. 2019. “Features of the Use of Modern Technology and Hardware at the Institute of Prosecution with the Aim of Prospering the Higher Education” In: International Journal of Higher Education. Vol. 8, No. 8, pp. 39-44.

ARTAMONOVA, Elena; KORNUKOV, Vladimir; RYABOVA, Liliya. 2021 “Observance of the Rights of Accused in the Conditions of Digitalization of Criminal Proceedings” In: Advances in Economics, Business and Management Research. Vol. 171, pp. 142- 147.

CARTER, Jeremy; GROMMON, Eric. 2015. “Officer perceptions of the impact of mobile broadband technology on police operations” In: Policing and Society. Vol. 27, No. 8, pp. 847-864.

CHURIKOVA, Anna; MANOVA, Nina; LAVNOV, Mikhail. 2021. Legal Mechanisms for Digitalization of the Activities of Prosecution Authorities. Available online. In: https://www.shsconferences.org/articles/shsconf/pdf/2021/04/shsconf_nid2020_02018.pdf. Consultation date: 15/04/2021.

COUNCIL OF EUROPE. 2020. Ukraine's hate crime, hate speech and discrimination data collection system. Recommendations for improvement and for adopting a joint approach and national situational analysis. Available online. In: https://rm.coe.int/final-data-collection-report-ukraine-en/16809fac70. Consultation date: 14/10/2020.

DE BLOK, Carolien; SEEPMA, Aline; ROUKEMA, Inge; VAN DONK, Dirk, Pieter; KEULEN, Berend; OTTE, Rinus. 2014. Summary. Digitisation in criminal justice chains. The experience in Denmark, England, Austria and Estonia from a supply chain perspective. Available online. In: https://www.rik.ee/sites/www.rik.ee/files/elfinder/article_files/14032-OPERA_English_Summary.pdf. Consultation date: 14/10/2020.

DELOITTE. 2015. The Digital Policing Journey: From Concept to Reality. Available online. In: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/public-sector/deloitte-uk-ps-digital-police-force.pdf. Consultation date: 17/10/2020.

EUAM UKRAINE. 2020. EU supports creation of state-of-the-art data centres to enhance National Police operations. Available online. In: https://www.euam-ukraine.eu/news/eu-supports-creation-of-state-of-the-art-data-centres-to-enhance-national-police-operations/. Consultation date: 15/10/2020.

FATIH, Tombul; BEKIR, Cakar. 2015. "Police use of technology to fight against crime" In: European Scientific Journal. Vol. 11, No.10, pp. 286-296.

GOODISON, Sean; DAVIS, Robert; JACKSON, Brian. 2015. Digital Evidence and the U.S. Criminal Justice System Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. Available online. In: https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf. Consultation date: 18/10/2020.

GUNDHUS, Helene; TALBERG, Niri; WATHNE, Christin. 2021. "From discretion to standardization: Digitalization of the police organization" In: International Journal of Police Science & Management. pp. 1-15.

HARKIN, Diarmaid; WHELAN, Chad; CHANG, Lennon. 2018. "The challenges facing specialist police cyber-crime units: an empirical analysis" In: Police Practice and Research. Vol. 19, No. 6, pp. 519-536.

ISHCHENKO, Petro. 2019. "Modern approaches to digitalization of pre-trial proceedings in criminal cases" In: Crime Cycle Sciences. Vol. 12, No. 157, pp. 68-79.

ISMAYLOV, Karen. 2017. "Educational and scientific establishment of the National police in ensuring cyber security strategy of Ukraine: the fundamental legal aspects" In: Center for European Reforms Studies. Vol. 4, pp. 25-29.

ISO. 2012. ISO/IEC 27037. Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. Available online. In: https://www.iso.org/standard/44381.html. Consultation date: 14/10/2020.

ISO. 2015a. ISO/IEC 27043. Information technology — Security techniques — Incident investigation principles and processes. Available online. In: https://www.iso.org/standard/44407.html. Consultation date: 17/10/2020.

ISO. 2015b. ISO/IEC 27041. Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method. Available online. In: https://www.iso.org/standard/44405.html. Consultation date: 18/10/2020.

ISO. 2015c. ISO/IEC 27042:2015. Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence. Available online. In: https://www.iso.org/standard/44406.html. Consultation date: 15/10/2020.

ISO. 2018 ISO/IEC 27050. Information technology — Security techniques — Electronic discovery. Available online. In: https://www.iso27001security.com/html/27050.html. Consultation date: 17/10/2020.

ISO. 2019. ISO/IEC 27050-1:2019. Information technology — Electronic discovery — Part 1: Overview and concepts. Available online. In: https://www.iso.org/standard/78647.html. Consultation date: 13/10/2020.

JANAKI, Mikaella. 2019. Digitalization of Investigation and Detection of Crime. Available online. In: https://www.academia.edu/33022605/Digitalization_of_Investigation_and_Detection_of_Crime. Consultation date: 14/10/2020.

MIJATOVIĆ, Dunja. 2019. Speech of Conference of Council of Europe Justice Ministers "Justice in Europe facing the challenges of digital technology". Available online. In: https://rm.coe.int/-justice-in-europe-facing-the-challenges-of-digital technology-speech-/16809835e0. Consultation date: 15/10/2020.

NORTJE, Jacobus Gerhardus; MYBURGH, Daniel Christoffel. 2019. "The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa" In: Potchefstroom Electronic Law Journal. Vol. 22, pp. 32- 75.

PRZHILENSKIY, Valeriy. 2020. "The Experience of Nature Mathematization in Criminal Proceedings Digitalization" In: Actual Problems of Russian Law. Vol. 15, No. 6, pp. 125-132.

SINCLAIR COTTER, Ryan. 2015. "Police intelligence: connecting-the-dots in a network society" In: An International Journal of Research and Policy. Vol. 27, pp. 173-187.

STELMAKH, Vladimir; EFREMOVA, Oksana; VASYUKOV, Viktor. 2021. Production of investigative actions aimed at obtaining and using computer information. Monograph. Available online. In: https://books.google.com.ua/books?id=3SxGEAAAQBAJ&printsec=frontcover&hl=ru#v=onepage&q&f=false. Consultation date: 17/04/2021.

STUBBS-RICHARDSON, Megan; COSBY, Austin; BERGENE, Karissa; COSBY, Arthur. 2018. Searching for safety: crime prevention in the era of Google. In: Crime Science. Vol. 7, pp. 21-34.

TAMBOVTSEV, Andrew; PAVLICHENKO, Natasha. 2021. Evolution of operational-search measures: monograph. Academy of Management of the Ministry of Internal Affairs of Russia. Moscow, Russia.

UNITED NATIONS. 2021. European Union provided Ukrainian Police with vehicles, state-of-the-art IT equipment and heavyduty bomb suit. Available online. In: https://ukraine.un.org/en/143836-european-union-provided-ukrainian-police-vehicles-state-art-it-equipment-and-heavy-duty-bomb. Consultation date: 17/04/2021.

VERKHOVNA RADA OF UKRAINE. 2004. Law of Ukraine "On Telecommunications". Available online. In: https://zakon.rada.gov.ua/laws/show/1280-15#Text. Consultation date: 17/10/2020.

VERKHOVNA RADA OF UKRAINE. 2010. Law of Ukraine "About the acquisition of personal tributes". Available online. In: https://zakon.rada.gov.ua/laws/show/2297-17#Text. Consultation date: 18/10/2020.

VERKHOVNA RADA OF UKRAINE. 2013. The Criminal Procedural Code of Ukraine. Available online. In: https://zakon.rada.gov.ua/laws/show/4651-17#Text. Consultation date: 14/10/2020.

VERKHOVNA RADA OF UKRAINE. 2020. Law of Ukraine "About promptly searching activity". Available online. In: https://zakon.rada.gov.ua/laws/show/2135-12/print. Consultation date: 15/10/2020.

WILSON-KOVACS, Dana. 2021. "Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales" In: Policing: An International Journal of Police Strategies and Management. Vol. 44, No. 4, pp. 669-682.

YEBOAH-OFORI, Antony; BROWN, Alan. 2020. "Digital Forensics Investigation Jurisprudence: Issues of Admis- sibility of Digital Evidence" In: Journal of Forensic, Legal & Investigative Sciences. Vol. 6, pp. 45-53.

UNIVERSIDAD
DEL ZULIA

CUESTIONES POLÍTICAS

Vol.39 Nº 71

Esta revista fue editada en formato digital y publicada en diciembre de 2021, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org