UDC 343
DOI: 10.32518/sals2.2024.162

The policy of rethinking the criminal process in the national security system: The impact of digitalisation on working with electronic evidence

Mishael Mohammad Alraggad

PhD in Law, Assistant Professor
Jadara University
21110, 733 P. O. Box, Irbid, Jordan
https://orcid.org/0000-0002-1846-8969

Ali Abd Alah Ali Almahasneh

PhD in Law, Assistant Professor
Jadara University
21110, 733 P. O. Box, Irbid, Jordan
https://orcid.org/0009-0006-7520-3592

Vitalina Borovikova

Scientific Researcher
Lviv State University of Internal Affairs
79007, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0003-4401-4562

Zinaida Zhyvko

Doctor of Economics, Professor
Institution of Higher Education "Private Joint-Stock Company
"Lviv Institute of Management"
79029, 16 Liska Str., Lviv, Ukraine
https://orcid.org/0000-0002-4045-669X

Yulia Komissarchuk*

PhD in Law, Associate Professor
Lviv State University of Internal Affairs
79007, 26 Horodotska Str., Lviv, Ukraine
https://orcid.org/0000-0002-5079-334X

Abstract. Choosing the right policy to rethink the criminal process is crucial for adapting and improving national security strategies to effectively counter and prevent new forms of crime that have evolved as a result of the impact of digitalisation. The purpose of the study was to form a modern scientific-methodological approach to choosing the optimal policy for adapting the criminal process to modern digitalisation factors. The key research methods were multi-criteria evaluation of alternatives, comparison of options by preference, and analysis using expert assessments. The innovation of the obtained research results was identified through an improved scientific-methodological approach to improving the effectiveness of the criminal process when working with electronic evidence. This approach differs from the existing ones due to its focus on the formation of alternative options in the choice of adaptation methods, providing an opportunity to choose the one that best meets the requirements of modern digitalisation. This approach focuses on flexibility and adaptability in developing procedures that allow effective interaction with electronic evidence while ensuring the high quality and speed of criminal proceedings. Due to the conducted study, it was established that for Ukraine, especially in the conditions of intensive digitalisation, the most effective is a flexible approach that involves adapting and rethinking

Suggested Citation **Article's History:** Received: 02.03.2024 Revised: 01.06.2024 Accepted: 26.06.2024

Alraggad, M.M., Almahasneh, A.A.A., Borovikova, V., Zhyvko, Z., & Komissarchuk, Yu. (2024). The policy of rethinking the criminal process in the national security system: The impact of digitalisation on working with electronic evidence. *Social & Legal Studios*, 7(2), 162-170. doi: 10.32518/sals2.2024.162.

*Corresponding author

traditional methods of criminal proceedings, considering the changing conditions and challenges posed by the digital era. The practical importance of the study results is expressed not only in the possibility of using them to develop strategies that will help the country adapt to the challenges of digitalisation but also in their meaningfulness for improving the effectiveness of responding to modern threats, such as cybercrime and other new forms of crime. These results can be used to develop comprehensive approaches to combating cybercrime, including improving legislative norms, improving methods for collecting and analysing electronic evidence, and improving the skills of law enforcement officers

Keywords: criminal procedure proceedings; digitalisation; use of electronic evidence; national security; cybercrime; modelling; comparison of options

Introduction

In a world where technological advances are relentless, traditional methodologies for criminal justice and evidence processing are constantly being questioned and often quickly become obsolete. In this regard, the digitalisation of criminal processes, especially in the skilful handling of electronic evidence, is crucial. The development of forensic science, especially digital forensics, is also crucial for the accurate interpretation and use of electronic evidence, which requires constant research and development in this area. New approaches to choosing a process implementation policy are needed that consider the challenges of digitalisation. Rethinking criminal proceedings in the context of national security and digitalisation is not only timely but also imperative. The dynamism of the external environment, characterised by rapid technological changes and the development of cyber threats, requires a flexible, effective, and legally reliable approach to the management of electronic evidence.

N. Chowdhury *et al.* (2022) examined cybersecurity training in Norwegian critical infrastructure companies. This study is particularly relevant because it sheds light on practical aspects of cybersecurity, an area of expertise needed to understand the challenges associated with processing electronic evidence within the framework of national security. J.A.A. Hammouri (2023) explores modelling the performance of criminal law functions in the context of security development. His investigation is directly related to the subject, as it delves into the practical aspects of adapting criminal law to modern security challenges, including those caused by digitalisation. In turn, B.M.A.-R. Tubishat *et al.* (2023) discuss the formation of an innovative model for the development of e-commerce as part of ensuring the economic security of business. Their understanding of e-commerce and digital platforms provides a unique perspective on the digital environment in which modern criminal processes operate. In turn, S. Nawaz *et al.* (2019) present an in-depth analysis of the online crime record management system. This study is particularly relevant for understanding how digital systems can be used to manage criminal cases, which is a central aspect of research on electronic evidence.

Notably, A. Natalis *et al.* (2023) explore the crucial role of the law in the development of human-environmental relations after COVID-19, with a particular focus on ecofeminism. Although their study is not directly related to digital evidence, it provides a broader context for understanding the changing role of law in society, especially in times of global change and crisis. Thus, the main gaps in the scientific literature related to the chosen subject of the study can be identified: lack of a unified vision of how to adapt the modern policy of implementing criminal proceedings; lack of specific actions to respond to the factors of digitalisation influence; lack of a clear vision of the model of working with electronic evidence in the framework of criminal proceedings; lack of use of adaptive approaches to solving the issue of rethinking criminal proceedings.

A study by A. Falade *et al.* (2019) focuses on a systematic review of crime prediction and data mining techniques. It highlights the importance of technological advances in crime prediction, a key aspect in adapting the criminal process to the demands of the digital age. R. Umar *et al.* (2018) focused on evaluating mobile forensics tools for investigating digital crimes. This assessment is key to understanding the effective inclusion of mobile electronic evidence in criminal investigations, an integral part of the digital transformation of the criminal justice system. A. Stepanyan *et al.* (2022) focused on the legal regime of scientific papers in the digital age, providing insight into the legal problems and frameworks that arise in connection with digitalisation.

A study by O. Sylkin *et al.* (2018) addresses the financial security of engineering enterprises as a prerequisite for the use of crisis management. This study, although indirectly, makes an important contribution to the broader discourse on the financial and resource aspects of digitalisation, in particular, in the context of adapting the criminal process. G.A.S. Atmaja and I.K.A. Mogi (2021) provides practical insights into digital evidence collection methodologies, particularly in cases of online fraud and focus on the use of the NIST method. Their findings are particularly relevant in the context of the evolution of cybercrime and its impact on national security. A paper of N. Hamad and D. Eleyan (2022) offers a comparative analysis of digital forensics tools used in cybercrime investigations. This analysis is essential for understanding the effectiveness and limitations of modern forensic tools in the digital age, providing an important insight into improving electronic evidence processing. Additionally, R. Mothukuri *et al.* (2020), discuss the use of the hybrid ANN-Shuffled frog leaping model to classify decisions in cybercrime cases. This innovative approach demonstrates the integration of advanced artificial intelligence techniques in the analysis and processing of digital evidence, highlighting an important step in the digital transformation of the criminal process.

Based on the results of the analysis of scientific literature and the examination of current trends in the field of digitalisation, the key purpose of this study was determined. It consists in the formation of a modern scientific-methodological approach to choosing the optimal policy for adapting the criminal process to modern digitalisation factors. Special emphasis is placed on the examination and analysis of the latest methods of processing and using electronic evidence in criminal cases, which is relevant both for Ukraine and international practice.

Materials and methods

The study presents a diverse number of methods that form the methodology and lay the foundation for the formation of a new approach to choosing the direction of policy development, rethinking the criminal process, and considering modern factors of digitalisation in the context of strengthening security development at the national level. In general, the research methodology includes: a method for analysing expert assessments to identify factors of influence; a method for multi-criteria evaluation of alternatives; a tabular and graphical method for displaying results; an abstract-logical method for forming conclusions; a method for comparing by preference of options.

The results of the study were visually determined using the graphical and tabular methods. In the course of the study, an approach was presented for choosing a policy for implementing criminal proceedings, and therefore, there was a need to present the factors that influence this choice. 30 experts from Ukraine were selected to determine them (10 practising lawyers; 10 active criminologists; 10 scientists in the field of criminal law) who, through the Google-questionnaire remote survey system, answered which factors in their opinion today in the context of digitalisation have the greatest impact on the criminal process and ensuring national security. Their responses were different and required to be normalised and structured (the group consensus assessment method or the group nominal consensus method helped with this in Zoom interviews). The Delphi method was used to form a single list of factors through a series of anonymous expert surveys. Firstly, the experts were sent questions which they answered, expressing their opinions and assessments. After each round, the responses were analysed, summarised, and sent back to the experts for review and reflection, considering the responses of other participants. This process was repeated several times until consensus or substantial stability of opinion was reached. The Delphi method allowed systematically integrating different standpoints, thus forming an objective and comprehensive understanding of the problem under study. The survey was conducted in the period September-November 2023. Ethical standards were observed during the survey. This means that participants were fully familiar with the study objectives, data collection methods, and ways to further use the information they received. The research was conducted in accordance with the rules of the Helsinki Declaration (1975).

The multi-criteria alternative evaluation method, also known as multi-criteria analysis, is a decision-making method used to evaluate a number of alternatives based on multiple criteria. This method is especially useful in situations where many different factors need to be considered, and complex aspects of a problem or choice need to be evaluated. The option preference comparison method is an important decision-making tool that allows assessing the relative importance or preference of various options or criteria. It starts by identifying all the options that need to be compared. In the future, each pair of options was compared with each other, and participants or experts were asked to rate which of the two options in each pair was better or more important using a rating scale. After collecting estimates for all pairs, the results were analysed, which allowed determining the relative importance of each variant. Therewith, the relativity scale was also used, in which certain factors are compared: 1 – factors are equal to each other; 2 – one factor has a small advantage; 3 – one factor has an advantage over another; 4 – one factor has a large advantage; 5 – one factor has an uncompromising advantage.

The limitations of the research are reflected in two aspects of the study. The list of factors influencing digitalisation is not exhaustive in nature and can be either reduced or expanded to consider new changes in the external environment. The research was conducted considering the specifics of the policy of introducing criminal proceedings in one country. Such restrictions may call into question the possibility of using the results obtained for other countries.

Results and discussion

The concept of "Criminal Procedure implementation policy" refers to the strategies and methods used by management and legislative bodies to reform and improve the criminal process. The introduction and development of the criminal process take place in the context of a balance between ensuring effective justice, protecting human rights and freedoms, and adapting to modern challenges and technologies. In each country, this process depends on specific legal traditions, cultural norms, and technological development. Therewith, it is affected by a different number of factors and threats. Based on the results of organising the opinion of experts through the Delphi method, the key factors of the digital age that influence the policy of introducing criminal proceedings were identified. The mathematical notation for them is represented through the symbol "EF" (Table 1).

Table 1. Factors of the digitalisation era that have a substantial impact on the policy of introducing criminal proceedings

EF	Impact factor	Characteristics
1	Electronic processing of evidence	The digitisation of evidence, such as digital documents, emails, and social media posts, has changed the way evidence is collected, stored, and analysed in criminal investigations. This requires new policies and tools to work with electronic evidence, ensure its authenticity, and protect it from falsification.
2	Data analytics for crime analysis	Digitalisation allows using sophisticated data analytics to analyse and predict crime. This includes the use of algorithms and artificial intelligence to analyse large data sets, which can help identify patterns, predict criminal activity, and aid in preventative police work.
3	Digital surveillance and monitoring	The use of digital surveillance and monitoring tools, including surveillance cameras, GPS tracking, and online activity monitoring, has expanded the capabilities of law enforcement agencies. This raises questions about privacy and civil liberties, requiring clear policies to balance the needs of law enforcement agencies with individual rights.
4	Online crime reporting and public relations	Digital platforms make it easier for the public to report crimes and expand interaction between law enforcement agencies and communities. This can lead to more effective crime reporting, but it also requires policies to manage and verify the receipt of digital information.

Table 1, Continued

EF	Impact factor	Characteristics
5	Cybercrime and digital forensics	With the rise of cybercrime, including hacking, online fraud, and identity theft, there is a growing need for expertise in digital forensics. Policymakers must adapt to combat these specialised crimes, including developing skills and tools to investigate and prosecute cybercrime.

Source: compiled by the authors

Further, it is necessary to present options for approaches to changing and rethinking the policy of introducing criminal proceedings. Therefore, there can be two of them ("GA"). The first is a stable approach to the policy of introducing criminal proceedings. The approach of adaptation to digitalisation is characterised by a more traditional and rigid position. Policies under this approach are updated less frequently and often lag behind rapid technological changes. There is a marked fluctuation in the adoption of new digital tools and technologies based on traditional methods of collecting evidence and investigating crimes. Digital problem-solving training programmes are minimal or outdated, and interaction with external stakeholders is limited, potentially leading to policies that are out of sync with technological advances and society's expectations. The legal framework for this approach tends to be rigid and does not fully consider the nuances and complexities associated with digital evidence and new types of cybercrime.

The second is a flexible approach to the policy of introducing criminal proceedings. It can be characterised by such traits as adaptability and foresight. It emphasises the importance of being aware of technological advances and digital trends. Key features include continuous policy development, active adoption of new technologies such as artificial intelligence and blockchain, and continuous training of lawyers to handle digital evidence and cybercrime effectively. It also involves working together with various stakeholders, including technology experts and privacy advocates, to ensure a balanced approach. Importantly, a legal framework based on a dynamic approach is designed to be flexible and able to consider new forms of digital evidence and cybercrime, ensuring a quick and effective legal response. The key task is to present an approach to selecting one of the criteria. Thus, it is necessary to present in detail the procedure for interaction between factors and selected policy options. Therefore, you can a task hierarchy can be formed (Fig. 1).

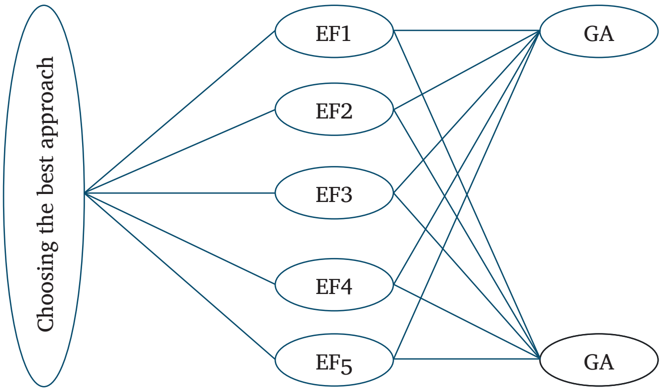

Figure 1. Hierarchy of tasks for choosing the optimal approach to the implementation of criminal proceedings under the influence of digitalisation

Source: compiled by the authors

Next, it is necessary to evaluate alternatives through respect for equality:

$$\frac{n*(n-1)}{2}, \qquad (1)$$

where n represents the number of digitalisation factors that influence the policy of introducing criminal proceedings (in the case of this study, there are 5 such factors). Then, when the adaptation approaches (GA) are already compared, a modified version of equality (1) will be used, namely:

$$n*\frac{m*(m-1)}{2}, \qquad (2)$$

where m represents the number of possible alternatives for each of the approaches (in the case of this study, there are also 5 such opportunities. This refers to 5 possible alternatives for the development of the influence of factors on the "GA" policy). Next, a matrix of comparisons of certain factors influencing digitalisation on the policy of implementing criminal proceedings is constructed, in which the diagonal is equal to one, and S is the sum of the elements of each column. A paired comparison matrix is created to evaluate elements at the same hierarchy level relative to a specific criterion. If there are n elements, the matrix will be n × n in size. Value 1: there are always units on the diagonal of the matrix because this reflects the comparison of the element with itself, which always has the same importance. A value higher than 1 (for example, 2, 3, ...) shows that the row element is considered more important than the column element. For example, a value of 2 means that a row element is twice as important as a column element. Fractional values (for example, 1/2, 1/3, ...). Indicate that the column element is more important than the row element. Thus, 1/2 means that the column element is twice as important as the row element (Fig. 2).

	EF1	EF2	EF3	EF4	EF5
EF1	1	1/2	1/3	1/4	4
EF2	2	1	4	1/2	3
EF3	3	1/4	1	4	2
EF4	4	2	3	1	5
EF5	1/4	1/3	1/2	1/5	1
S	0.11	0.26	0.14	0.4	0.06

Figure 2. Matrix of comparisons of certain factors influencing digitalisation on the policy of implementing criminal proceedings

Source: compiled by the authors

Further, it is necessary that there is consistency between the opinions and assessments of the experts involved. The value of λmax, which is used to determine the consistency coefficient, is determined to do this:

$$\mathrm{IU} = \frac{\lambda\mathrm{max} - n}{n-1}. \qquad (3)$$

In the examined case, IU = 0.03. Next, WU (the level of inconsistency should be below 10%) is determined via IU/WI, where WI is 1.12 (a number from the table of randomness values, if 5 factors, then 1.12). In the case of this study, it is 3%, which indicates the validity of experts' judgments. Such a comparison allows determining whether the differences between experts are substantial, or whether they are within an acceptable level of randomness. If the level of inconsistency exceeds the established threshold, this may indicate the need to review expert assessments or conduct additional rounds of surveys to achieve greater consensus. Next, it is necessary to compare the proposed approaches with the increased influence of each of the factors. Since there will be 5 such cases, one example of calculation can be presented in detail in the study, and other intermediate calculations will be outside the text (Fig. 3).

	GA1	GA2
GA1	1	2
GA2	1/2	1
S	0.6	0.4

Figure 3. Matrix of comparisons of proposed approaches to changing the policy of implementing criminal proceedings according to the scenario of development of the EF1 factor

Source: compiled by the authors

Then, when for each EF criterion, the matrix was represented as in the case of Figure 3, it becomes possible to determine the priority of one of the proposed approaches to adapting the policy of introducing criminal proceedings in the context of digitalisation and the impact of its factors:

$$\mathrm{U} = \sum_{i=1}^{n} s * u. \qquad (4)$$

$U_1 = 0.3$. $U_2 = 0.6$, which demonstrates that the most optimal approach to the policy of implementing criminal proceedings is to adapt this process to new technologies. Thus, it can be seen that there is a need to adapt the most sensitive among the processes, namely, working with electronic evidence. In this regard, it is necessary to present a modern mechanism for improving the work with electronic evidence, considering the proposed approach to choosing the optimal adaptation policy.

Thus, the proposed mechanism demonstrates a comprehensive approach to the implementation of criminal proceedings in the context of ensuring national security, with an emphasis on working with electronic evidence. It provides for determining the optimal way to introduce changes in the criminal process, updating the role of electronic evidence in this context. The mechanism described includes improved legislation and improved technical equipment for law enforcement agencies, which work together to strengthen procedures for processing electronic evidence.

Firstly, the way how the results of the study improve the theoretical basis for a given problem should be discussed. The study provides a detailed understanding of how digitalisation affects the criminal process. By integrating the methods of multi-criteria assessment, comparison of advantages and analysis of expert assessments, it is possible to obtain a comprehensive structure that surpasses traditional approaches. It enriches theoretical discourse by offering a more holistic view of the challenges and opportunities that digitalisation opens up in the criminal justice system. The practical application of the findings in the field of electronic evidence management fills a critical gap in the literature, where previous theories have often focused on the conceptual aspects of digitalisation without fully considering its practical implications in the form of real-world factors of influence. Thus, the study provides a new, effective approach that can be directly applied to improving the criminal process, thereby increasing the practical usefulness of existing theoretical models. Consequently, the theoretical understanding of digital evidence was expanded, going beyond traditional data types and covering a wider range of digital traces. This expansion is crucial in an era where digital evidence can range from online communications to sophisticated data analysis, contributing to a more comprehensive and inclusive theoretical framework that can consider the evolving nature of digital evidence. It is submitted using the corresponding model in the study (Fig. 4).

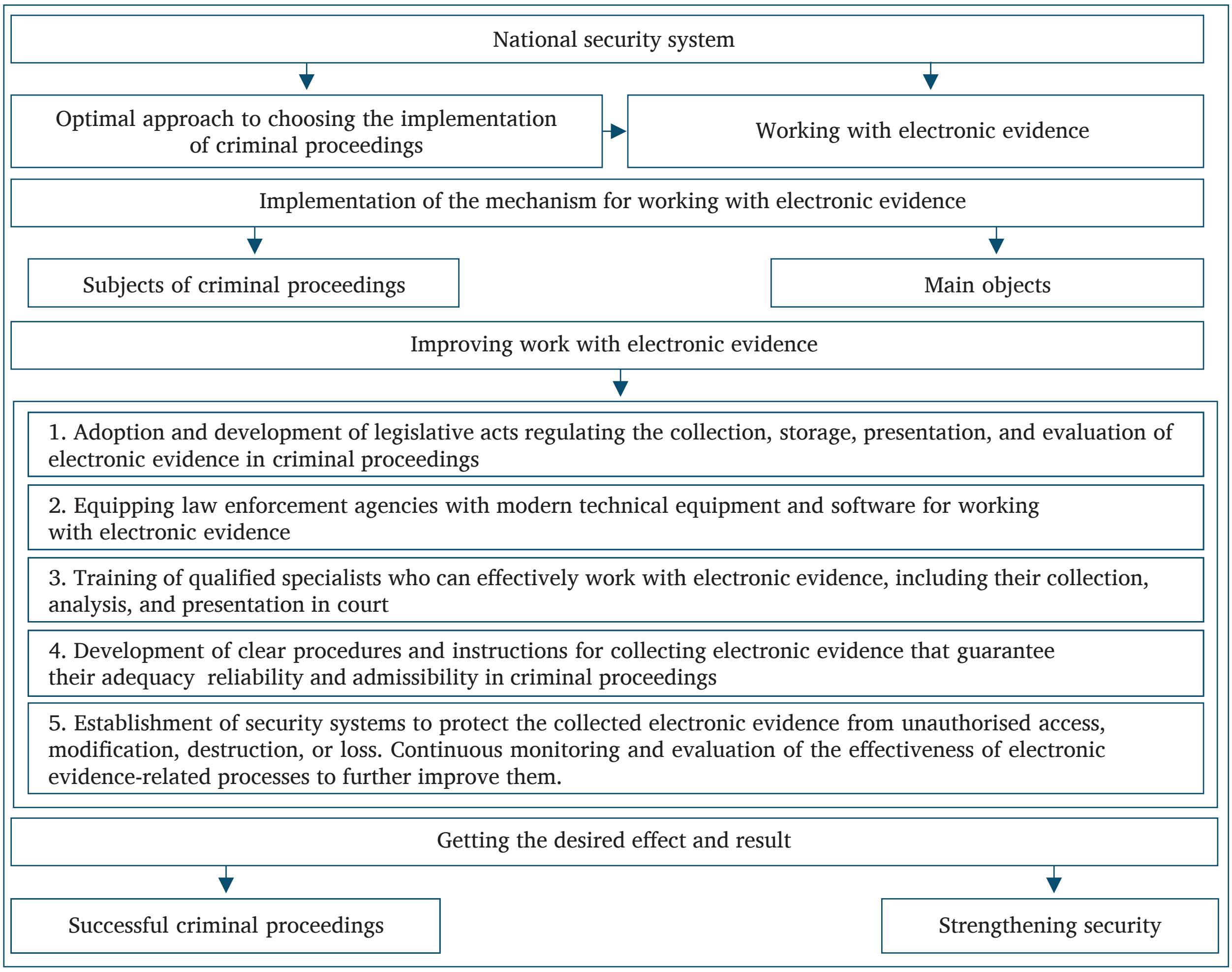
National security system
Optimal approach to choosing the implementation of criminal proceedings
Working with electronic evidence
Implementation of the mechanism for working with electronic evidence
Subjects of criminal proceedings
Main objects
Improving work with electronic evidence
1. Adoption and development of legislative acts regulating the collection, storage, presentation, and evaluation of electronic evidence in criminal proceedings
2. Equipping law enforcement agencies with modern technical equipment and software for working with electronic evidence
3. Training of qualified specialists who can effectively work with electronic evidence, including their collection, analysis, and presentation in court
4. Development of clear procedures and instructions for collecting electronic evidence that guarantee their adequacy reliability and admissibility in criminal proceedings
5. Establishment of security systems to protect the collected electronic evidence from unauthorised access, modification, destruction, or loss. Continuous monitoring and evaluation of the effectiveness of electronic evidence-related processes to further improve them.
Getting the desired effect and result
Successful criminal proceedings
Strengthening security

Figure 4. The modern mechanism for improving work with electronic evidence, considering the proposed approach to choosing the optimal adaptation policy

Source: compiled by the authors

When discussing the results obtained, it is necessary to compare them with similar ones in this direction. For example, a study by F.A.F. Alazzam *et al.* (2023) highlights the need for an adapted and legally appropriate digital platform structure, drawing a parallel with the claim that criminal proceedings should be flexible but reliable in dealing with electronic evidence. Their focus on information models in e-commerce provides a useful analogy for how criminal justice systems should develop their information processing processes, especially in the field of electronic evidence.

Methodological approach of A.R. Harutyunyan (2021) to the prevention of crimes against political rights offers a prism through which it is possible to consider the methods. This philosophical-legal approach provides a deeper understanding of the ethical and legal difficulties associated with adapting the criminal process, especially in a politically tense and digitally interconnected world. A paper of T.F. Shih *et al.* (2019) on the cloud-based crime reporting system is consistent with conclusions about the need for innovative digital solutions in criminal proceedings. Their focus on protecting personal data in this digital framework overlaps with the focus of this study on balancing technological progress with individual rights and privacy concerns.

An investigative audit by S. Susanto and E. Purwanto (2023) in environmental affairs demonstrates the specialised application of digital techniques in legal scenarios, reiterating the claim of this study that criminal proceedings must be adapted to different forms of digital evidence for different types of crimes. A study by A.S. Padmanabhan and S. Sapna (2022) in DNA profiling and data exchange highlights the growing importance of international collaboration in the context of digital evidence. This aspect highlights the emphasis of this study on the need to adapt the criminal process not only within national borders but also in the international arena. A. Hisham *et al.* (2021) demonstrate the practical application of digitalisation in criminal proceedings in crime record management systems, which is consistent with the findings of this study on the need for efficient and adaptable systems for managing electronic evidence. Ultimately, the definition of the digital shadow economy given by R. Remeikiene *et al.* (2018) and P. Pylypyshyn *et al.* (2022) provides context for the study, highlighting the nature of emerging crime in the digital age and the resulting need for a criminal process capable of coping with the complexities of using electronic evidence.

Thus, within the framework of the discussion part of the study, there are key differences inherent in the results of the examination: an approach to improving the formation of a policy of rethinking the criminal process based on the influence of digitalisation factors is presented; two approaches to improving/rethinking the criminal process based on the principles of adaptation under the influence of digitalisation are proposed; a model of flexible access to the introduction of the criminal process and work with electronic evidence is proposed. This study complements and expands on the results of previous studies. Focusing on flexible and sustainable approaches is necessary to contribute to improving criminal procedure implementation policies, which will not only address current digital challenges but also enable national security to evolve in line with future technological advances. This adaptability is critical to shaping appropriate national security policies and the effective administration of justice in an increasingly digital world.

Conclusions

As a result, it should be noted that the results obtained for the current purpose of the study do not exhaust this subject. Evidently, this area of research remains deeply relevant and critical, especially given the current state of war and the growing role of artificial intelligence in criminal investigations. Notably, the key result of the study is the presented approach, which has a number of characteristic innovative provisions and principles. In addition, digitalisation factors were identified that have a substantial impact on the policy of introducing criminal proceedings and ensuring national security. Thus, the scientific-methodological approach to improving the effectiveness of the criminal process when working with electronic evidence was improved. Therewith, two radically different approaches to the policy of implementing the criminal process are proposed: a flexible approach that focuses on continuous improvement and updating of the criminal process in accordance with changing conditions and challenges; a stable approach that focuses on preserving existing norms and procedures of the criminal process. It emphasises the importance of stability and predictability in the legal system, minimising frequent changes and helping to avoid uncertainty in the legal field. As a result of the assessment and modelling, it was determined that in the current conditions of digitalisation and current work with electronic evidence, the most optimal approach to the policy of implementing criminal proceedings, which will make the process of ensuring security possible.

Key areas for further research can be identified. There is a need to investigate the impact of digital warfare and cybercrime on national security strategies. This research should focus on identifying new forms of digital threats, understanding their consequences, and developing a legal and procedural framework to effectively address them. Moreover, the role of international cooperation in the fight against digital crime may be a critical area of future research. This includes examining the effectiveness of existing international legal instruments, understanding the challenges of cross-border digital evidence collection, and proposing a framework for International cooperation and information exchange.

Acknowledgements

None.

Conflict of interest

None.

References

[1] Alazzam, F.A.F., Shakhatreh, H.J.M., Gharaibeh, Z.I.Y., Didiuk, I., & Sylkin, O. (2023). Developing an information model for E-Commerce platforms: A study on modern socio-economic systems in the context of global digitalization and legal compliance. *Ingénierie des Systèmesd Information*, 28(4), 969-974. doi: 10.18280/isi.280417.

[2] Atmaja, G.A.S., & Mogi, I.K.A. (2021). Acquisition of digital evidence in online scam cases (CyberCrime) on Whatsapp chat application using NIST method. *JELIKU*, 9(4) 511-518. doi: 10.24843/jlk.2021.v09.i04.p08.

[3] Chowdhury, N., Nystad, E., Reegard, K., & Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. *International Journal of Safety and Security Engineering*, 12(3), 299-310. doi: 10.18280/ijsse.120304.

[4] Falade, A., Azeta, A., Oni, A., & Odun-ayo, I. (2019). Systematic literature review of crime prediction and data mining. *Review of Computer Engineering Studies*, 6(3), 56-63. doi: 10.18280/rces.060302.

[5] Hamad, N., & Eleyan, D. (2022). Digital forensics tools used in cybercrime investigation-comparative analysis. *Journal of Xi'an University of Architecture & Technology*, 4, 113-127. doi: 10.37896/JXAT14.04/314909.

[6] Hammouri, J.A.A. (2023). Modeling the performance of criminal law functions in the context of safety and security development. *International Journal of Safety and Security Engineering*, 13(3), 395-401. doi: 10.18280/ijsse.130302.

[7] Harutyunyan, A.R. (2021). International methodological basics of electoral law (From antiquity to modern times: Philosophy-legal dimension). *Wisdom*, 2(18), 103-113. doi: 10.24234/wisdom.v18i2.496.

[8] Hisham, A., Ahmed, A., Khaled, M., Abdullatif, N., & Kassem, S. (2021). Modelling of crime record management system using unified modeling language. *Ingénierie des Systèmes d'Information*, 26(4), 365-373. doi: 10.18280/isi.260404.

[9] Mothukuri, R., Basaveswararao, B., & Bulla, S. (2020). Judgement classification using hybrid ANN-Shuffled frog leaping model on cyber crime judgement database. *Revue d'Intelligence Artificielle*, 34(4), 445-456. doi: 10.18280/ria.340409.

[10] Natalis, A., Purwanti, A., & Asmara, T. (2023). The law s critical role in developing human-environment relationships after COVID-19 pandemic (a study of ecofeminism*)*. *International Journal of Safety and Security Development and Planning*, 18(1), 153-160. doi: 10.18280/ijsdp.180116.

[11] Nawaz, S., Ghaffar, J., Siddique, A., & Aslam, M. (2019). On-line crime records management system. *Information Engineering and Applications*, 9(6), 11-20. doi: 10.7176/JIEA/9-6-02.

[12] Padmanabhan, A.S., & Sapna, S. (2022). A study on DNA profiling techniques and transnational exchange of DNA data from databank. *Revue d'Intelligence Artificielle*, 36(3),427-438. doi: 10.18280/ria.360310.

[13] Pylypyshyn, P., Hanushchyn, S., Bek, U., Mykhalitska, N., & Veresklia, M. (2022). Legal regulation of the financial and economic security of Ukraine. *Financial and Credit Activity Problems of Theory and Practice*, 1(42), 510-521. doi: 10.55643/fcaptp.1.42.2022.3747.

[14] Remeikiene, R., Gaspareniene, L., & Schneider, F.G. (2018). The definition of digital shadow economy. *Technological and Economic Development of Economy*, 24(2), 696-717. doi: 10.3846/20294913.2016.1266530.

[15] Shih, T.F., Chen, C.L., Syu, B.Y., & Deng, Y.Y. (2019). A cloud-based crime reporting system with identity protection. *Symmetry-Basel,* 11(2), article number 255. doi: 10.3390/sym11020255.

[16] Stepanyan, A., Manukyan, E., Tevosyan, L., & Ilyushina, M. (2022). Legal regime for scientific works in the digital age. *Wisdom,* 21(1), 117-122. doi: 10.24231/wisdom.v21i1.625.

[17] Susanto, S., & Purwanto, E. (2023). Investigative auditing in environmental pollution cases: An analysis of Indonesian supreme court decision. *International Journal of Sustainable Development and Planning*, 18(11), 3673-3678. doi: 10.18280/ijsdp.181134.

[18] Sylkin, O., Shtangret, A., Ogirko, O., & Melnikov, A. (2018). Assessing the financial security of the engineering enterprises as preconditions of application of anti-crisis management: Practical aspect. *Business and Economic Horizons*, 14(4), 926-940. doi: 10.15208/beh.2018.63.

[19] The Declaration of Helsinki. (1975, October). Retrieved from https://www.wma.net/what-we-do/medical-ethics/declaration-of-helsinki/.

[20] Tubishat, B.M.A.-R., Alazzam, F.A.F., Savchenko, O., Pitel, N., & Diuk, O. (2023). Formation of an innovative model for the development of e-commerce as part of ensuring business economic security. *Business: Theory and Practice*, 24(2), 594-603. doi: 10.3846/btp.2023.19781.

[21] Umar, R., Riadi, I., & Zamroni, G.M. (2018). Mobile forensic tools evaluation for digital crime investigation. *International Journal on Advanced Science Engineering and Information Technology*, 8(3), 949-955. doi: 10.18517/ijaseit.8.3.3591.

Політика переосмислення кримінального процесу в системі забезпечення національної безпеки: вплив цифровізації на роботу із електронними доказами

Мішаель Мохаммад Алраггад

Кандидат юридичних наук, доцент
Університет Джадара
21110, а/с 733, м. Ірбід, Йорданія
https://orcid.org/0000-0002-1846-8969

Алі Абд Алах Алі Альмахасне

Кандидат юридичних наук, доцент
Університет Джадара
21110, а/с 733, м. Ірбід, Йорданія
https://orcid.org/0009-0006-7520-3592

Віталіна Боровікова

Науковий співробітник
Львівський державний університет внутрішніх справ
79007, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0003-4401-4562

Зінаїда Живко

Доктор економічних наук, професор
Вищий навчальний заклад «Приватне акціонерне товариство
«Львівський інститут менеджменту»
79029, вул. Ліська 16, м. Львів, Україна
https://orcid.org/0000-0002-4045-669X

Юлія Коміссарчук

Кандидат юридичних наук, доцент
Львівський державний університет внутрішніх справ
79007, вул. Городоцька, 26, м. Львів, Україна
https://orcid.org/0000-0002-5079-334X

Анотація. Вибір вірного політичного курсу в питанні переосмислення кримінального процесу має вирішальне значення для адаптації та вдосконалення стратегій національної безпеки для ефективної протидії та запобігання новим формам злочинності, які еволюціонували внаслідок впливу цифровізації. Метою статті було формування сучасного науково-методичного підходу до вибору оптимальної політики адаптування кримінального процесу до сучасних чинників цифровізації. Ключові методи дослідження – метод багатокритеріальної оцінки альтернатив, метод порівняння за перевагою варіантів, метод аналізу за допомогою експертних оцінок. Інноваційність отриманих результатів дослідження розкривається через удосконалений науково-методичний підхід до покращення ефективності кримінального процесу при роботі із електронними доказами. Цей підхід відрізняється від існуючих завдяки своєму зосередженню на формуванні альтернативних варіантів у виборі методів адаптації, надаючи можливість обрати той, який найкраще відповідає вимогам сучасної цифровізації. Основна увага в цьому підході приділяється гнучкості та адаптивності в розробці процедур, які дозволяють ефективно взаємодіяти з електронними доказами, забезпечуючи при цьому високу якість та швидкість кримінального процесу. Завдяки проведеному дослідженню було виявлено, що для України, особливо в умовах інтенсивної цифровізації, найбільш ефективним є гнучкий підхід, який передбачає адаптування та переосмислення традиційних методик кримінального процесу з урахуванням змінюваних умов і викликів, що ставить цифрова ера. Практична значущість отриманих результатів дослідження виражається не лише у можливості їх використання для розробки стратегій, що сприятимуть адаптації країни до викликів цифровізації, але й у їх значущості для підвищення ефективності відповіді на сучасні загрози, такі як кіберзлочинність та інші новітні форми злочинності. Ці результати можуть бути використані для розробки комплексних підходів у боротьбі з кіберзлочинами, включаючи вдосконалення законодавчих норм, поліпшення методів збору та аналізу електронних доказів, а також підвищення кваліфікації правоохоронців

Ключові слова: кримінальне процесуальне судочинство; діджиталізація; використання електронних доказів; національна безпека; кіберзлочинність; моделювання; порівняння варіантів