



RESEARCH ARTICLE

Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations

Dmytro Patreliuk¹, Ivo Svoboda*², Inha Kalancha³, Vadym Filashkin⁴, Bohdan Kachmar⁵

¹LAW FIRM «Dmytro Patreliuk», Kyiv, Ukraine.

²AMBIS, a.s. Vyská škola, Praha, Česká Republika.

³Department of Public Law, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine.

⁴Department of Criminalistics and Forensic Medicine, National Academy of Internal Affairs, Kyiv, Ukraine.

⁵Department of National Security, Interregional Academy of Personnel Management, Kyiv, Ukraine.

ARTICLE INFO

ABSTRACT

Received: Jul 24, 2024

Accepted: Sep 13, 2024

Keywords

Criminal investigations

Cybersecurity, digital technologies, databases

Transnational crime

Legal evidence base

***Corresponding Author:**

svoboda21ivo@gmail.com

The relevance of using electronic systems is growing in the context of the globalisation of transnational crime. The article aims to analyse the potential applications of these systems to identify possible areas for their improvement. The research methodology is based on identifying the current state of the crime rate in the world and its trends, as well as a technical review of electronic systems for continuous operation. The study results show that digital technologies speed up the process of sharing evidence, reduce the risk of its loss or distortion, and contribute to the transparency and accountability of investigations. The article highlights the main challenges related to cybersecurity. The proposed ways to overcome these challenges include the development of international standards, advanced training of law enforcement officers, and introducing the latest tools. The practical significance of the article lies in its ability to formulate recommendations on implementing effective electronic evidence exchange systems adapted to the specifics of different legal systems, thereby contributing to the transparency and accountability of investigations. Further research should focus on new technologies' impact and implementation in international investigative practice.

INTRODUCTION

Solving international crimes is one of the biggest challenges for modern law enforcement agencies. According to Miller (2023), transnational crimes are characterised by a high level of organisation and mobility of criminals, which makes them difficult to detect and apprehend. The diversity of legal systems creates additional obstacles to effective law enforcement. Successfully solving such crimes requires not only highly qualified personnel but also access to modern technologies and tools that allow the processing of large amounts of information. This underscores the critical need for strengthening law enforcement agencies, a task that requires significant training and equipment investment.

International law enforcement cooperation is a critical element in the fight against transnational crime. The authors Thakkar et al. (2023) believe that interaction between law enforcement agencies of different countries, coordination of joint operations and information exchange is essential to counter global threats successfully. INTERPOL, Europol and the UN play an important role in creating platforms for cooperation, providing mechanisms for intelligence sharing and coordination at a

confidential level. International cooperation requires harmonising legal standards and procedures, allowing for a rapid response to criminal acts, regardless of geographical location. This process includes the conclusion of bilateral and multilateral agreements, joint exercises, and professional training for law enforcement officers.

Digital technologies are leading in modern investigations, providing law enforcement agencies with the tools to collect, process and analyse evidence effectively. According to Nosál (2023), electronic systems significantly speed up the investigation process and reduce the likelihood of errors or loss of essential data. Modern evidence management systems provide automated recording and tracking of all stages of evidence handling, increasing the investigation process's transparency and accountability. The introduction of machine learning opens up opportunities for identifying and analysing complex criminal activity. This technology allows law enforcement to identify suspects accurately, analyse large amounts of data and draw reasonable conclusions based on the evidence.

The study aims to analyse the effectiveness of electronic systems for the international exchange of evidence in criminal investigations and to compare them with the European experience. The article identifies the main objectives: 1. to assess the effectiveness of existing electronic systems for exchanging evidence in criminal investigations. 2. To identify the peculiarities of protecting confidential information while exchanging evidence between countries. 3. To study the trends in introducing the latest digital technologies in criminal investigations. 4. To develop recommendations for improving evidence exchange procedures based on the experience of European countries.

LITERATURE REVIEW

The issue of using electronic systems for the international exchange of evidence in criminal investigations is a subject of broad debate in the scientific community. Researchers study various aspects of their impact on the efficiency and transparency of criminal investigations. The authors Gupta and Husain (2023) examine the role of electronic systems in improving communication between law enforcement agencies in different countries, emphasising the importance of investigation processes. The study by Casino et al. (2022) analyses the impact of digital technologies on protecting confidential information and cybersecurity in the exchange of evidence. In his article, Gannon et al. (2023) discuss the benefits of using automated evidence management software. The author El-Kady (2023) highlights the experience of European countries in implementing electronic evidence exchange systems, noting their contribution to improving the effectiveness of law enforcement. Mesarčík et al. (2023) emphasise the importance of international cooperation and harmonisation of legal standards for successfully integrating digital technologies into the investigation process. Zavydniak (2021) analyses law enforcement agencies' challenges in implementing electronic systems. Stoykova and Franke (2023) draw attention to the role of new technologies in ensuring transparency and accountability of investigation processes. Murachov (2023) explores the impact of digital evidence-sharing platforms on improving coordination between different jurisdictions. According to Okmi et al. (2023), an important aspect is improving law enforcement officers' skills working with electronic systems through regular training and education programmes. The study Cinar and Bharadiya (2023) emphasises the need to develop and implement international standards to ensure effective information exchange between countries. Rojszczak (2020) examines the challenges related to cybersecurity and data protection when using electronic systems. The article by Ombu (2023) discusses the mechanisms of evidence exchange in the fight against international crime, emphasising the peculiarities of integrating international standards into national legal systems. Lukić-Radović and Manojlović-Nedeljković (2023) emphasise the significance of expanding the application of digital technologies to enhance the efficiency of law enforcement agencies. The potential for expanding opportunities for public involvement in monitoring and controlling compliance with the law in criminal investigations is an insufficiently explored issue. Kosta and Kamara (2023) and Melnyk et al. (2022) emphasise the importance of international

projects and programmes to improve the exchange of evidence between countries. Sharma et al. (2023) analyse the shortcomings of implementing electronic systems regarding privacy and legal regulation. Martin (2021) and Mulska et al. (2022) confirm that applying a systematic approach to the management of electronic evidence has allowed for the successful implementation of large-scale projects in the field of criminal investigations. Machado and Granja (2019) highlight the challenges and problems law enforcement agencies face in evidence sharing in the context of growing international tensions and cyber threats. Consequently, scholars call for developing a flexible legal framework to support and regulate digital technologies' use in criminal investigations. Given the limited number of studies, it is necessary to continue developing this research issue at the local and regional levels.

METHODOLOGY

Research procedure

The research methodology studies the potential use of electronic systems in the context of the growing number of criminal investigations. First, the research procedure includes identifying the most dangerous countries with high crime rates that pose a significant threat to global security. The next step is to assess the functionality of existing electronic evidence exchange systems to identify strengths and weaknesses. The final step is to determine the potential impact of these systems on how different countries use technology to fight international crime.

Sampling

The study sample was formed based on the highest level of use of electronic systems for the exchange of evidence in countries with a high crime rate. The sample includes countries actively implementing e-Evidence Digital Exchange Systems, the European Investigation Order Platform and others. These systems were selected because of their significant impact on the international exchange of evidence efficiency in criminal investigations. The regions analysed are Saint Kitts and Nevis, Jamaica, Saint Vincent and the Grenadines, Turks and Caicos Islands, Ecuador, Lesotho, Saint Lucia, Haiti, Belize, Trinidad and Tobago, South Africa and Nigeria. They were chosen due to their high crime rates (based on official statistics on crime rates and the use of electronic systems) and the active use of digital technologies in law enforcement.

Methods

The research methods include statistical analysis of data from law enforcement systems, a methodology for assessing the effectiveness of digital technologies through secondary analysis, and a comparative analysis of international standards and protocols for evidence sharing. Quantitative analysis includes statistical methods to determine crime rates and the effectiveness of evidence sharing, while qualitative analysis provides insight into the mechanisms behind these indicators. Secondary and content analysis is used to examine official reports, legislation, and academic publications relating to the use of electronic systems in criminal investigations.

Tools

Research tools include Excel data analysis software. Content analysis is carried out using NVivo data processing tools, ensuring efficient processing of vast quantities of data and recognising essential trends and patterns. The use of these tools provides the accuracy and reliability of the results obtained, allowing us to draw reasonable conclusions and recommendations for improving the systems of evidence exchange in criminal investigations at the international level.

RESULTS

Today, the rise in crime is one of the most pressing issues affecting the security and stability of the international environment. According to the United Nations, the number of cybercrime cases has

increased by 600% over the past decade, underscoring modern technology's importance in combating these threats. The instability in the global international environment caused by political conflicts, economic crises and environmental disasters is contributing to the growth of criminal groups. According to the World Bank, conflicts and violence cost the global economy approximately USD 14.3 trillion annually, about 12.6% of global GDP. In such circumstances, the effective functioning of international legal mechanisms becomes critical to ensuring global security.

The rise of terrorism and other forms of extremism is a significant concern in the international arena. Terrorist organisations continue to carry out attacks around the world, causing panic and instability in society. According to the Global Terrorism Index, the number of terrorist attacks increased by 22% in 2024 compared to the previous year. This indicator highlights the need for close international cooperation for effective information exchange and coordination between countries. Recording crimes and sharing evidence in real time are critical elements in the fight against various forms of international crime. INTERPOL and Europol already play an essential role in the investigation process by providing platforms for intelligence sharing and operations coordination. However, to achieve a higher level of effectiveness, these systems need to be continuously improved by introducing the latest technologies and developing new methods to combat global threats. The countries with the highest crime rates are shown in Figure 1.

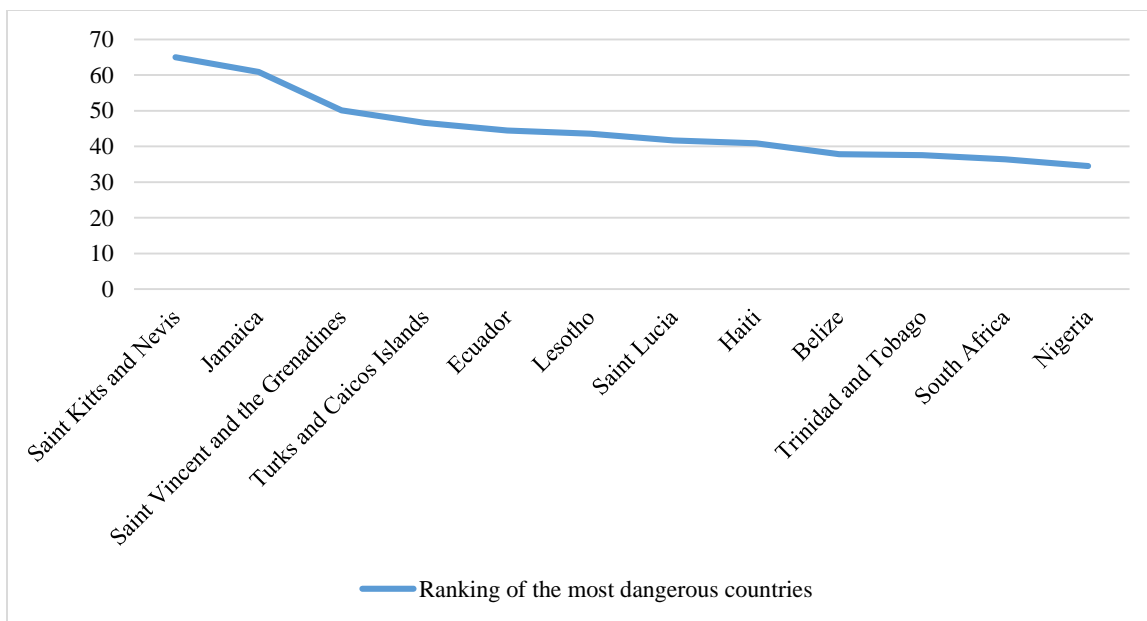


Figure 1. Ranking of the most dangerous countries in the world in 2023 by murder rate (per 100,000 inhabitants)

Source: compiled based on Statista data

Specialised systems play a vital role in exchanging data to form an evidence base in criminal investigations. One of these systems is electronic databases, which allow law enforcement agencies to store, process and exchange large amounts of information in digital format. The ECRIS (European Criminal Records Information System) system provides for the rapid exchange of information on criminal records between the EU countries. It allows automated querying and retrieval of information on citizens' criminal records, significantly reducing data processing time and improving information accuracy. Technical features include data encryption standards, multi-level access systems and automated mechanisms for updating information, ensuring high security and confidentiality.

International cooperation in data exchange to form an evidence base is also significantly enhanced by introducing digital platforms and specialised systems. Interpol uses the I-24/7 system, rapidly exchanging information on crimes, suspects and stolen items. It operates around the clock, allowing law enforcement agencies from different countries to exchange information in real-time. Using secure communication technologies and standardised data formats ensures the reliability and efficiency of such systems, facilitating a rapid response to international crimes. Based on open data, the functionality of these systems is presented in Table 1 using the method of technical analysis.

Table 1. Characteristics of the functionality of electronic systems for international exchange of evidence

Electronic system	Characteristics	Functionality
e-Evidence Digital Exchange System (needs)	A system designed to facilitate the exchange of electronic evidence between EU countries.	Increases the speed and efficiency of evidence exchange; reduces data security risks.
European Investigation Order (EIO) Platform	A platform for exchanging requests and evidence under the European Investigation Order.	Promotes greater consistency and standardisation of the evidence exchange process; facilitates interaction between different jurisdictions.
Secure Information Exchange Network Application (SIENA)	The system, operated by Europol, is designed to enable the secure exchange of information between law enforcement agencies in the EU and other international partners.	It provides a high level of security for information transmission and supports a wide range of types of evidence and information.
Schengen Information System (SIS)	An information system that supports exchanging information on offenders and wanted persons among Schengen countries.	It improves the coordination of law enforcement agencies in the fight against transnational crime and provides prompt access to critical information.
Interpol's I-24/7	Interpol's global communication system for the secure exchange of information between law enforcement agencies worldwide.	Enhances global cooperation between law enforcement agencies; enables rapid exchange of critical information.

Source: compiled by the author

Technological innovations open up new opportunities to improve data exchange in criminal investigations. They are used to ensure the integrity and transparency of evidence by creating secure and unalterable records of all activities during the investigation. Forming an evidence base in criminal investigations requires standardised procedures to ensure the admissibility of evidence in court. The specifics of this process include the need to collect, store and process evidence in a manner that guarantees its integrity and protection from unauthorised access or manipulation.

For this purpose, various digital tools are used, such as evidence management systems, which automate the processes of cataloguing, storing and transferring evidence. For example, the Chain of Custody system provides detailed documentation of each stage of evidence processing, including information about the persons who had access to the evidence and the time and place of its collection and transfer. Cryptography and blockchain technology further enhance security by ensuring data

integrity and protection against forgery. Modern systems allow for integrating various types of evidence, from physical to digital, providing a comprehensive approach to investigations.

The growth of crime on different continents is a severe problem that requires new strategies and approaches to detect and combat it effectively. In the United States, the crime rate remains high despite slight fluctuations in statistics. According to the Federal Bureau of Investigation (FBI), in 2023, the number of violent crimes increased by 5.6% compared to the previous year. In Europe, especially in Western countries, there is an increase in the number of cases of organised crime and terrorism. In 2021, the number of reported terrorist attacks in France increased by 18%. In Asia, especially in Southeast Asia, the rise in crime is linked to human and drug trafficking. According to the UN, the number of human trafficking cases in this region has increased by 25% over the past five years. In Africa, due to political instability and armed conflicts, crime remains critically high, requiring international support for effective law enforcement. The general trend in crime rates by region is shown in Table 2.

Table 2. Criminality scores by continent, 2023

Region	Criminality		Criminal markets		Criminal actors		Resilience	
Asia	5,47	+0,18	5,41	+0,20	5,53	+0,15	4,34	-0,12
Africa	5,25	+0,08	5,05	+0,11	5,45	+0,05	3,85	+0,05
Americas	5,20	+0,13	4,89	+0,19	5,51	+0,08	4,80	-0,03
Europe	4,74	+0,26	4,60	+0,40	4,88	+0,12	6,27	+0,04
Oceania	3,23	+0,16	3,28	+0,30	3,19	+0,02	5,55	+0,09
Global average	5,03	+0,16	4,88	+0,22	5,19	+0,09	4,81	-0,00

Source: calculated based on Ocindex data

Increased migration flows significantly impact the growth of crime related to the exploitation and discrimination of migrants worldwide. According to the International Organisation for Migration (IOM), the number of international migrants is growing by an average of 3.6% annually and tends to increase yearly. In such circumstances, criminal groups use migrants' vulnerability to organise illegal activities. This situation requires new approaches to detecting and investigating crimes from law enforcement agencies.

Cybercrime is a new and rapidly evolving trend that requires specialised approaches to detect and prevent crimes in the digital space. The main types of cybercrime include financial fraud, ransomware attacks, phishing and unauthorised access to confidential information. Digital crimes are global and are committed by organised criminal groups operating in different countries. To effectively combat cybercrime, it is necessary to develop new technological solutions, such as systems for monitoring and analysing cyber threats, and to implement international cybersecurity standards. Cooperation between the public and private sectors is essential to share information and better coordinate efforts to combat cybercrime.

International organisations are vital to building the evidence base for fighting transnational crime. Europol uses the SIENA (Secure Information Exchange Network Application) system to exchange intelligence securely and coordinate joint investigations between EU countries. It supports standardised data exchange formats and ensures high data protection. Through the United Nations provides technical assistance and training to law enforcement agencies in its member states, promoting the implementation of international standards and best practices in investigations. The joint efforts of these organisations aim to ensure consistency of legal approaches, improve the efficiency of information exchange and strengthen global security through the reliable generation and use of evidence.

DISCUSSION

The study found that using electronic systems for the international exchange of evidence significantly increases the efficiency of criminal investigations. This aligns with the findings of Rusman et al. (2023), who emphasise the importance of digital technologies for protecting confidential information and cybersecurity. The study by Dulskyi et al. (2023) confirms our findings on the reduced risk of data loss or distortion through automated evidence management systems. However, Lee and Lim (2023) note that the unification of protocols and procedures for information exchange between countries remains a challenge that requires further work. Cubitt et al. (2023) emphasise the importance of harmonising legal standards to improve international law enforcement cooperation, which is consistent with our findings. Fitzpatrick and Donnelly (2021) confirm the importance of legal collaboration through digital platforms to exchange evidence between different jurisdictions. The article by Simmler et al., (2023) emphasises the use of international standards to ensure the effective exchange of evidence about the need to harmonise legal procedures. Tudorica and Bonnici (2023) emphasise the importance of international projects to improve the exchange of evidence. The study by Moussa (2021) focuses on privacy and legal regulation, confirming the conclusions about the challenges associated with implementing electronic systems. An alternative view is expressed by Chetry and Sharma (2023), who emphasise the human factor's potential to improve the evidence-sharing process. The study by Sulisdyantoro and Marzuki (2023) dwells on the importance of law enforcement training for effectively using electronic systems. A comparison of the results with those of other researchers shows the need to invest in cybersecurity infrastructure, harmonisation of legal standards, and training for effective international evidence exchange. The study's objective was to assess the effectiveness of electronic systems for the international exchange of evidence in criminal investigations, which was successfully achieved. The study's results confirmed that the data obtained meet the objectives of implementing electronic systems in international cooperation. Based on this, it is recommended that these systems should be introduced into national legal practices to optimise international cooperation.

CONCLUSION

Thus, the author identifies the main aspects of using electronic systems for international exchange of evidence in the transnational legal system. It is substantiated that solving international crimes requires significant efforts on the part of law enforcement agencies due to the complexity of their organisation and the high level of mobility of criminals. The analysis shows that international cooperation and coordination between jurisdictions are integral to successful transnational crime investigations. The article considers the role of digital technologies in ensuring the effective exchange of evidence, which allows for faster investigation and increased accountability. Modern evidence management systems, databases and information exchange platforms are critical elements in enhancing the effectiveness of law enforcement.

Despite the significant benefits of implementing electronic systems, significant drawbacks require attention. One of the main challenges is ensuring cybersecurity and protecting confidential information when exchanging evidence between different countries. The growing number of cybercrimes and the risk of unauthorised access to sensitive data underscore the need to develop robust security systems. The second challenge is the harmonisation of legal standards and procedures between different jurisdictions, which complicates the process of international cooperation. There is also the problem of underfunding and insufficient training of personnel who must work with the latest technologies. These challenges require a comprehensive approach and active cooperation at the international level to overcome them. The findings can be used to improve legal frameworks and procedures for international evidence exchange, with the prospect of future research to assess their impact on different jurisdictions and criminal justice systems.

Recommendations

Based on the study, the author proposes the following measures to ensure the legal activities of jurisdictions in global cooperation:

1. Ensure the development and implementation of reliable data protection systems that guarantee the security of evidence exchange between law enforcement agencies of different countries.
2. Establish standard protocols and procedures to harmonise the legal aspects of evidence exchange between different jurisdictions.
3. Introduce modern evidence management systems that provide automated recording, tracking and analysis of evidence, increasing transparency and accountability of the investigation process.

REFERENCES

- Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A. and Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence, *Journal of Cybersecurity*. Oxford University Press, 8(1), tyac014. <https://doi.org/10.1093/cybsec/tyac014>
- Chetry, A. and Sharma, U. (2023). Anonymity in decentralised apps: Study of implications for cybercrime investigations, *International Journal of Experimental Research and Review*, 32, 195–205. <https://doi.org/10.52756/ijerr.2023.v32.017>
- Cinar, B. and Bharadiya, J. P. (2023). Cloud computing forensics; Challenges and future perspectives: A review, *Asian Journal of Research in Computer Science*, 16(1), 1–14. <https://doi.org/10.9734/ajrcos/2023/v16i1330>
- Cubitt, T. I. C., Napier, S. and Brown, R. (2023). Understanding the offline criminal behavior of individuals who live stream child sexual abuse, *Journal of Interpersonal Violence*, 38(9-10), 6624–6649. <https://doi.org/10.1177/08862605221137712>
- Dulskiy, O., Leliuk, T., Luhovyi, V., Melnyk, V. and Morgun, I. (2023). International cooperation when collecting evidence in the investigation of transnational organised crime: Challenges and opportunities, *Revista Amazonia Investiga*, 12(70), 88–101. <https://doi.org/10.34069/ai/2023.70.10.8>
- El-Kady, R. M. (2023). Handling E-evidence in Egyptian and comparative legislation: A comparative analytical study, *Arab Journal of Forensic Sciences and Forensic Medicine*, 5(2), 191–222. <https://doi.org/10.26735/WGZY6322>
- Fitzpatrick, R. W. and Donnelly, L. J. (2021). An introduction to forensic soil science and forensic geology: A synthesis, *Geological Society Special Publication*, 492, 1–32. <https://doi.org/10.1144/SP492-2021-81>
- Gannon, C., Blokland, A. A. J., Huikuri, S., Babchishin, K. M. and Lehmann, R. J. B. (2023). Child sexual abuse material on the darknet, *Forensische Psychiatrie, Psychologie, Kriminologie*, 17(4), 353–365. <https://doi.org/10.1007/s11757-023-00790-8>
- Gupta, G. and Husain, A. (2023). Digital evidence in police investigation: A comparative analysis of challenges faced in India, the UK and the United States, *Journal of Victimology and Victim Justice*, 6(2). <https://doi.org/10.1177/25166069231184977>
- Kosta, E. and Kamara, I. (2023). The Right to an effective remedy in international data transfers of electronic evidence: Past lessons and future outlook, *Review of European Administrative Law*, 16(1), 57–83. <https://doi.org/10.7590/187479823X16800083010356>
- Lee, S. and Lim, G.-C. (2023). A review on the direction of legislative improvement of electronic information offshore seizure and search, *Wonkwang University Legal Research Institute*, 39(1), 113–135. <https://doi.org/10.22397/wlri.2023.39.1.113>
- CLukić-Radović, M. and Manojlović-Nedeljković, M. (2023). Effectiveness of the joint investigation team as an instrument for gathering and exchange of evidence in cross-border investigations,

- Zbornik Radova Pravnog Fakulteta Nis*, 62(100), 93–124. <https://doi.org/10.5937/zrpfno-46661>
- Machado, H. and Granja, R. (2019). Police epistemic culture and boundary work with judicial authorities and forensic scientists: the case of transnational DNA data exchange in the EU, *New Genetics and Society*, 38(3), 289–307. <https://doi.org/10.1080/14636778.2019.1609350>
- Martin, C. (2021). Treaty-based regulation and evidence-extradition agreements as critical tools in the fight against international criminal wrongdoing, *International Criminal Law Review*, 22(5-6), 1168–1187. <https://doi.org/10.1163/15718123-bja10085>
- Melnyk, D. S., Parfyo, O. A., Butenko, O. V., Tykhonova, O. V. and Zarosylo, V. O. (2022). Practice of the member states of the European Union in the field of anti-corruption regulation, *Journal of Financial Crime*, 29(3), 853–863. <https://doi.org/10.1108/JFC-03-2021-0050>
- Mesarčík, M., Podroužek, J. and Gavorník, A. (2023). On defence of “ethification” of law: How ethics may improve compliance with the EU digital laws, *Computer Law and Security Review*, 50, 105852. <https://doi.org/10.1016/j.clsr.2023.105852>
- Miller, C. M. (2023). A survey of prosecutors and investigators using digital evidence: A starting point, *Forensic Science International: Synergy*, 6, 100296. <https://doi.org/10.1016/j.fsisyn.2022.100296>
- Moussa, A. F. (2021). Electronic evidence and its authenticity in forensic evidence, *Egyptian Journal of Forensic Sciences*, 11(1), 20. <https://doi.org/10.1186/s41935-021-00234-6>
- Mulska, O., Vasylytsiv, T., Shushkova, Y., Kloba, L. and Parfenyuk, Y. (2022). Assessment of the population's social resilience environment (the case of the Carpathian Region of Ukraine), *Problems and Perspectives in Management*, 20(1), 407–421. [https://doi.org/10.21511/ppm.20\(1\).2022.33](https://doi.org/10.21511/ppm.20(1).2022.33)
- Murachov, R. (2023). Features of the organisation of interaction between the international criminal court and law enforcement structures of Ukraine regarding the investigation of crimes, *Analytical and Comparative Jurisprudence*, 6, 692–696. <https://doi.org/10.24144/2788-6018.2023.06.119>
- Nosál, J. (2023). Crime in the digital age: A new frontier. In *The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network* (pp. 177–193). Springer International Publishing. https://doi.org/10.1007/978-3-031-24673-9_11
- Okmi, M., Por, L. Y., Ang, T. F., Al-Hussein, W. and Ku, C. S. (2023). A systematic review of mobile phone data in crime applications: A coherent taxonomy based on data types and analysis perspectives, challenges, and future research directions, *Sensors. MDPI*, 29(9), 4350. <https://doi.org/10.3390/s23094350>
- Ombu, A. (2023). Role of digital forensics in combating financial crimes in the computer era, *Journal of Forensic Accounting Profession*, 3(1), 57–75. <https://doi.org/10.2478/jfap-2023-0003>
- Rojszczak, M. (2020). CLOUD act agreements from an EU perspective, *Computer Law and Security Review*, 38, 105442. <https://doi.org/10.1016/j.clsr.2020.105442>
- Rusman, G., D’orio, E., Popova, E. and Kipouras, P. (2023). Features of the application of digital technology in criminal proceedings of the BRICS countries, *BRICS Law Journal*, 10(1), 35–58. <https://doi.org/10.21684/2412-2343-2023-10-1-35-58>
- Sharma, P., Kumar, M. and Sharma, H. (2023). Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: An evaluation, *Multimedia Tools and Applications*, 82(12), 18117–18150. <https://doi.org/10.1007/s11042-022-13808-w>
- Simmler, M., Brunner, S., Canova, G. and Schedler, K. (2023). Smart criminal justice: Exploring the use of algorithms in the Swiss criminal justice system, *Artificial Intelligence and Law*, 31(2), 213–237. <https://doi.org/10.1007/s10506-022-09310-1>

- Stoykova, R. and Franke, K. (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations, *Forensic Science International: Digital Investigation*, 45, 301554. <https://doi.org/10.1016/j.fsidi.2023.301554>
- Sulisdyantoro, D. and Marzuki, M. I. (2023). Identification of Whatsapp digital evidence on Android smartphones using the Android backup APK (application package Kit) downgrade method, *Journal of Integrated and Advanced Engineering (JIAE)*, 3(1), 7–22. <https://doi.org/10.51662/jiae.v3i1.70>
- Thakkar, P., Patel, D., Hirpara, I., Jagani, J., Patel, S., Shah, M. and Kshirsagar, A. (2023). A Comprehensive review on computer vision and fuzzy logic in forensic science application, *Annals of Data Science. Springer Science and Business Media Deutschland GmbH*, 10, 761–785. <https://doi.org/10.1007/s40745-022-00408-6>
- Tudorica, M. and Bonnici, J. M. (2023). Legal framework for digital evidence following the implementation of the EIO directive: Status quo, challenges and experiences in member states. In *Law, Governance and Technology Series* (pp. 127–151). Springer Nature. https://doi.org/10.1007/978-3-031-31686-9_9
- Zavydniak, I. (2021). Subjects of interaction and the level of its support in investigation of economic crimes of a transnational character, *Evropsky Politicky a Pravni Diskurz*, 8(6), 56–62. <https://doi.org/10.46340/eppd.2021.8.6.9>