Articles

Studia Iuridica Lublinensia vol. 33, 5, 2024
DOI: 10.17951/sil.2024.33.5.57-67

Zsanett Fantoly
University of Szeged, Hungary
ORCID: 0000-0003-1016-0377
fantoly@juris.u-szeged.hu

Simplifying Criminal Proceedings Using Artificial Intelligence in Criminal Compliance*

Uproszczenie postępowania karnego z wykorzystaniem sztucznej inteligencji w procesie criminal compliance

ABSTRACT

Countries quickly realized that simplifying and speeding up criminal proceedings were essential to increase efficiency. The development of a cooperation system with the prosecution and the related introduction of new legal instruments are the latest achievements of the legislative processes of the last decades. It is also the case of criminal compliance, which allows a company to be actively involved in an investigation and assists the investigating authority to obtain certain benefits in criminal proceedings in return for its cooperation (e.g. not to be charged or to receive a significantly lighter sentence). The emergence of artificial intelligence offers new opportunities for all institutions of society, including jurisprudence. This paper explores the potential application of AI in the context of criminal compliance.

Keywords: criminal compliance; artificial intelligence; criminal proceeding

CORRESPONDENCE ADRESS: Zsanett Fantoly, PhD, Prof. Dr. Habil., Full Professor, University of Szeged, Faculty of Law, Department of Criminal Sciences, Bocskai u. 10-12, 6722 Szeged, Hungary.

* The research was supported by the Digital Society Competence Centre of the Humanities and Social Sciences Cluster of the Centre of Excellence for Interdisciplinary Research, Development and Innovation of the University of Szeged. The author is a member of the "Artificial Intelligence and the Legal Order" research group.

INTRODUCTION

As early as 1987, Recommendation R(87)18 of the Committee of Ministers of the Council of Europe[1] listed several ways of simplifying criminal proceedings, from investigation through prosecution to trial. Although the right (and the obligation) to investigate criminal conduct lies exclusively with the State, the possibility for the accused to cooperate with law enforcement authorities in criminal proceedings to establish substantive justice is now recognized by law in almost all countries. Many forms of cooperation with the prosecution are accepted in the criminal procedure codes of different nations. However, for all of them, the emergence of artificial intelligence (AI) brings new opportunities for the defendant who chooses to cooperate with the authorities involved in the criminal justice system. By AI we mean the ability to think creatively and deductively, including primarily learning, by machines and the programs and algorithms behind the entities that run them, enabling the machines to make decisions autonomously.[2] The difference between AI and traditional computers is that while a computer makes a decision based on a known "if-then" relationship, i.e. it is pre-programmed with a possible answer, AI can develop knowledge that has not been pre-programmed by its developers so that it can react from an almost infinite number of possibilities.[3] Artificial intelligence is understood at the system level: a system embedded in software-based or hardware tools that simulates intelligence behavior by, among other things, collecting and processing data, analyzing and evaluating its environment, and acting in a somewhat autonomous way to achieve specific goals.[4]

The application of AI in criminal proceedings is expected to filter and deter specific types of crime (e.g. human trafficking, sexual exploitation of children, money laundering, cybercrime or terrorism), to improve the working methods of the authorities in criminal matters and to contribute to the efficiency of decision-making by law enforcement authorities. Artificial intelligence systems also

[1] Recommendation No. R(87)18 of the Committee of Ministers to Member States concerning the simplification of criminal justice of the Council of Europe, adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies. The text of the Recommendation is available at https://rm.coe.int/16804e19f8 (access: 11.12.2024).

[2] B. Marr, *The Complete Beginners' Guide to Artificial Intelligence*, 25.4.2017, https://www.forbes.com/sites/bernardmarr/2017/04/25/the-complete-beginners-guide-to-artificial-intelligence/?sh=fda0e364a835 (access: 10.12.2024); I. Ambrus, K. Mezei, E. Molnár, *Magyarázat a compliance jogszabályairól I. Általános és büntetőjogi compliance*, Budapest 2021, p. 447.

[3] L. Staffer, O. Jany, *Künstliche Intelligenz und Strafrechtsflege – eine Orientierung*, "Zeitschrift für Internationale Strafrechtsdogmatic" 2020, vol. 15(4), pp. 164–167; Cs. Herke, *A mesterséges intelligencia kriminalisztikai aspektusai*, "Belügyi Szemle" 2021, vol. 69(10), p. 1711.

[4] Committee on Legal Affairs, Report on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)).

have autonomous decision-making competences in performing expert tasks and work significantly faster than traditional human resources.[5]

The motion for a resolution of the European Parliament on AI in criminal law and its use by police and judicial authorities in criminal matters lists areas where AI can be a valuable tool in criminal investigations, including various facial recognition technologies, DNA profiling, automated number plate recognition and searching suspect/defendant databases. Thera are also included speech recognition by algorithms, various technologies for reading lips and post-hearing surveillance (shot detection algorithms), as well as AI activities developed through the search and analysis of identified databases, predictive (i.e. predictive policing and crime hot trace analysis), behavioral monitoring tools and tools for identifying financial fraud and terrorist financing. Social media surveillance (i.e. data collection for data mining links) and automated surveillance systems with different detection capabilities (e.g. heart rate monitoring or thermal cameras) also must be addressed.[6]

In particular, using AI in cooperation with law enforcement authorities is worthwhile for large companies and legal entities with international activities and a dominant role in market competition, where an inadequate organizational culture allows the commission of criminal offenses within the company, sometimes using it. Nowadays, some companies are seriously trying to build up internal investigation and control methods in criminal compliance activities. For them, cooperation with the public law enforcement authorities to investigate the crime and gather evidence is rewarding if the subsequent criminal sanctions that may be imposed are reduced or even waived by the authorities given the cooperation.

The present study demonstrates the potential of the use of AI in criminal proceedings and e-discovery processes in internal investigations for defendants and legal entities that prefer to cooperate with the authorities.

ARTIFICIAL INTELLIGENCE AND CRIMINAL COMPLIANCE IN INVESTIGATIONS

Criminal compliance refers to the measures that can be taken in the corporate sphere to avoid criminal law violations and, as a consequence, criminal prosecution or specialization,[7] or, in the case of a crime already committed, to investigate, evaluate

[5] K. Karsai, *Algorithmic Decisions within the Criminal Justice Ecosystem and Their Problem Matrix*, "International Review of Penal Law / Revue Internationale de Droit Penal" 2021, vol. 92(1), p. 18.

[6] Committee on Civil Liberties, Justice and Home Affairs, Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).

[7] T. Rotsch, *Criminal Compliance*, Baden-Baden 2015; I. Ambrus, K. Mezei, E. Molnár, *op. cit.*, pp. 50–51.

and determine the organizational response to a series of offenses, or to contact the authorities in charge of criminal matters in order to initiate criminal proceedings.[8] One of the instruments of criminal compliance is an internal investigation, a control procedure within an organization to investigate and evaluate a past event, in this case, the event that gave rise to the criminal offense. An internal investigation is, therefore, an organizational response to the suspicion of a criminal offense, which is the repressive aspect of criminal compliance.[9] It is worthwhile for the company to invest financial resources in the internal investigation because its willingness to cooperate after the offense has been committed may result in exemption from criminal liability by the criminal authorities or in a significant reduction in the level of the penalty imposed. In the case of detection of the infringement, collection of evidence supporting the infringement and its transmission to the investigating authority, or cooperation with law enforcement authorities, the criminal sanction may be replaced, on a case-by-case basis, by an intra-company sanction, with no prosecution.[10] In addition, an initial investigation may also have a crime-preventive effect, i.e. it may prevent further offenses from being committed within the legal person. Indeed, if it is clear to the company's managers and employees that their wrongdoing will be detected in an internal investigation, they will likely refrain from committing it.[11]

In corporate criminal compliance, AI can be used in prevention (through early case assessments), review (through ex-post case studies), and collect and evaluate the facts and evidence that determine individual cases.[12] In particular, the latter algorithm application technique can be helpful for the investigating authority in terms of accepting the willingness of the accused to cooperate. The embedded AI helps to filter and classify data content according to specific criteria, automatically identifying concepts and the documents that can be associated with them. The data can come from various sources; facts and information stored on servers in banks, financial institutions, hospitals, etc. can be scrutinized.[13] Data can be extracted, collected and

[8] I. Ambrus, Á. Farkas, *A compliance alapkérdései. Az etikus vállalati működés elmélete és gyakorlata*, Budapest 2019, p. 207.

[9] C. Momsen, *Internal Investigations zwischen arbeitsrechtlicher Mitwirkungspflicht und strafprozessualer Selbstbelastungsfreiheit*, "Zeitschrift für Internationale Strafrechtsdogmatik" 2011, vol. 6(6), p. 11; I. Ambrus, K. Mezei, E. Molnár, *op. cit.*, p. 446.

[10] E. Molnár, *A vállalkozáson belüli előnyomozási eljárás interdiszciplináris kontextusban*, "Jogtudományi közlöny" 2016, vol. 71(9), p. 460.

[11] Zs. Fantoly, Cs. Herke, B. Szabó, *The Role of AI-based Systems in Negotiated Proceedings*, "e-Revue Internationale de Droit Penal" 2023, vol. 17, https://www.penal.org/de/2023-2 (access: 10.12.2024).

[12] T. Knierm, *Erfordennise und Grenze der Internal Investigation*, [in:] *Wissenschafliche und praktische Aspekte der nationalen und internationalen Compliance-Diskussion*, Baden-Baden 2010, p. 81.

[13] S.H. Schneider, M. Priewer, *LegalTech: Solutions to Old and New Challenges in Internal Investigations*, 2020, https://www.financierworldwide.com/legaltech-solutions-to-old-and-new-challenges-in-internal-investigations#.Y3DkTnbMI2w (access: 10.12.2024).

analyzed by the AI. In addition to revealing the interrelationship between individuals and organizations, so-called advanced analytics can also be used for sentiment analysis, i.e. to select documents by tone or topic. Process analysis, in turn, suggests a model for achieving more efficient performance and filtering out risk factors.[14] For example, using Casepoint Advanced Analytics, it has been reported that the algorithm was used to conduct an internal audit of a multi-billion dollar international company for only $200,000 and two weeks, which would have been simply unfeasible to do so cost-effectively and in such a short time using manual tools.[15] The international company would have had to collect and criminally assess 60,000 documents, mainly in Japanese, within two weeks. Budget constraints and an unrealistic deadline presented a significant challenge, as in addition to analyzing and evaluating documents in foreign languages, knowledge of the local legal framework was essential to assess the activities of a multinational company operating in several countries. By running the algorithm purchased by the multinational company, a keyword search of the company's correspondence system for its managers and employees in both English and Japanese was made possible. Translation and local lawyer's and legal adviser's fees, which would have represented a significant part of the criminal costs in a possible criminal prosecution, were completely eliminated as a result of the internal investigation using the algorithm. From a financial point of view, it is, therefore, clearly worthwhile for the prosecution to accept the defendant's offer that the company involved in the criminal proceedings will hand over to the law enforcement authorities the evidence obtained by the AI during its internal investigation. It will save costs and time for the authorities and help increase the investigation's efficiency. Furthermore, the accurate and rapid collection and processing of vast amounts of unstructured data (such as video footage, images, emails and other text files), cognitive data analysis not only contributes to the effectiveness of the investigation but is also of crucial importance from a preventive point of view not to mention the fact that manual data processing and evaluation cannot exclude the risk elements of human factors, such as errors due to bias.[16]

At the same time, cooperation also benefits the suspect or the legal person involved in the offense. Although, in the absence of men's rea, the criminal codes

[14] A. Bellapu, *Artificial Intelligence is Playing a Big Role in Fraud Investigation*, 2.4.2021, https://www.analyticsinsight.net/artificial-intelligence-is-playing-a-big-role-in-fraud-investigation (access: 11.12.2024).

[15] Of the 60,000 documents originally covered, only 600 remained in the filter after the keyword search. See Casepoint, *How a Multi-Billion Dollar Corporation Reaped Major Cost Savings Conducting an Internal Investigation Using Casepoint*, https://www.casepoint.com/resources/case-studies/corporte-ediscovery-cost-savings-artificial-intelligence (access: 11.12.2024).

[16] N. Carrington, *How Forensic Investigators Gain an Edge with AI*, 22.10.2018, https://www2.deloitte.com/ch/en/pages/forensics/articles/forensic-investigators-gain-an-edge-with-ai.html (access: 11.12.2024).

of the continental European countries, which have been brought up on traditional criminal law doctrine, exclude the guilt and, therefore, the criminal liability of the legal person, most national legislations allow for the imposition of specific penalties in criminal proceedings and, more importantly, the application of criminal law measures against the legal person involved in the offense. Typically, this is possible in cases where a legal person's manager or a member of its supervisory board commits a criminal offense using the legal person, such as cartel offenses, fraud, money laundering, etc. In such cases, the detection of unlawful conduct within the company is not only worthwhile for the legal person because of the lighter (or even waived) sanction in exchange for cooperation but also because of the shorter period the legal person is subject to criminal proceedings, the less damage to its entrepreneurial prestige.[17]

If relevant data concerning the persons identified by the investigating authority are collected and filtered by AI-driven means, voluntary fact-finding, and data provision may be essential aspects of cooperation to facilitate unrestricted mitigation of the sanction. In the U.S., the so-called Filip Factors have already been developed, which provide a summary of the criteria on which the prosecution decides whether to prosecute (or terminate) a legal person in a particular case about the criminal compliance activities of the enterprise.[18] Among these considerations, in the section on "Confidential Reporting and Investigation", we find questions urging the use of AI in corporate internal investigations, such as "Does the company have an effective way of collecting and analyzing allegations of misconduct?".[19] Although the purchase of AI tools and their application within the established legal framework requires a significant financial investment for companies, it is worthwhile for the legal entity, as compliance with a cooperation agreement based on the use of AI may result in immunity from prosecution or at least a significantly reduced sanction.

Of course, the use of criminal compliance and AI is not geographically specific to the United States of America, but as we can see, perhaps as a consequence of globalization, widespread all over the world, therefore it is present in Europe as well. Whereas common law legal systems and specifically the U.S. case law is more reactive and flexible towards technological innovation and changes on a case-by-case precedent basis, most European continental legal systems rely on acts and statutory criminal procedure legislation. This legislative framework either needs to be abstract or specific enough to respond well and to include electronic data as types of new evidence, such as information retrieved from virtual voice assistants.

[17] Zs. Fantoly, Cs. Herke, B. Szabó, *op. cit*.

[18] S.H. Schneider, M. Priewer, *op. cit*.

[19] Strategic Management Services, *Evaluating Corporate Compliance Programs Using the DOJ "Filip Factors"*, June 2018, https://www.compliance.com/resources/evaluating-corporate-compliance-programs-using-the-doj-filip-factors (access: 11.12.2024).

In Hungary, at the time of the submission of this article, we are currently unaware of any precedents comparable to this American example introduced above, therefore our account in the following is limited to the review of the relevant provisions of the Hungarian Criminal Procedure Act (CPA) and the EU framework. The Hungarian CPA in § 165 (a) lists electronic data as a specific type of evidence. Electronic data is defined in § 205 as any representation of facts, information or concepts in a form suitable for processing by an IT system, including software suitable to cause a computer system to perform a function. This is also in line with the definition of "computer date" provided for by the Budapest Convention on Cybercrime in Article 1 (b): "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function. As for the retrieval of data and electronic evidence, the CPA allows the following national procedures: undercover collection of open-source data (§ 215 (2) and § 215 (5) (b) CPA); data request (§ 261 CPA); search and seizure (§§ 302, 308 and 315 CPA); seizure and order to preserve electronic data (§§ 315–316 CPA); secret surveillance of IT systems including both traffic and content data (§ 231 (a) CPA); wiretapping, including both traffic and content data (§ 231 (e) CPA).[20]

Carrying out these prosecutorial actions requires a significant investment of energy and money on the part of the authorities. However, with criminal compliance, the company concerned voluntarily provides the relevant electronic data to the investigating authority and the prosecution, thus simplifying the process of gathering and processing evidence.

Criminal compliance can also be used in investigations against multinational companies. However, additional principles must be considered, mainly when electronic data stored in online devices constitute evidence.

When it comes to judicial cooperation in criminal matters, as for the admissibility of data gathered via direct requests to foreign based online service provider as evidence, according to the Eurojust SIRIUS 2nd Annual Report, the Hungarian national legal framework does not specifically allow, nor forbids direct data requests from abroad. Should it still happen in praxis (e.g. upon police information gathering based on the existing criminal procedure framework) with the data eventually being sent, the authors argue that it would not constitute a breach of law or harm of legal status of the procedural parties and therefore could be used in evidence.[21] Although

[20] Zs. Fantoly, A. Lichtenstein, *Siri, Alexa and Co. in the Criminal Justice System: The Use of Virtual Voice Assistants in Criminal Investigation and Their Admissibility as Digital Evidence*, [in:] *Digital Criminal Justice: A Studybook*, Istanbul 2023, https://eta.bibl.u-szeged.hu/5804 (access: 10.12.2024).

[21] SIRIUS, *SIRIUS EU Digital Evidence Situation Report: 2nd Annual Report*, 2020, https://www.eurojust.europa.eu/publication/sirius-eu-digital-evidence-situation-report-2020 (access: 10.12.2024), p. 17.

the argument seems well founded, based on the level of protection of procedural rights provided by the Hungarian CPA, we believe that some relevant Hungarian cases and jurisdiction are still needed to support this claim.[22]

The SIRIUS Report also claims that Hungarian domestic online service providers are generally not allowed to respond to direct requests from foreign authorities. According to the findings of the project, they are constantly being monitored by the National Security Service to prevent any foreign illegal and malicious access to Hungarian communications infrastructure. In conclusion, it is reported to seem unlikely that an Online Service Provider would respond to such order even though it is not *expressis verbis* forbidden or regulated clearly.[23]

If the data subject consents to the disclosure of their data, the cross-border direct request is possible in Hungarian regard. This is also said to be a standard practice implemented by the police.[24]

The criminal justice authorities must enforce certain procedural safeguards when cooperating with the defendant. The legal rules and regulations governing internal investigations are constantly changing and cover various areas of law (e.g. labor law, health rules, data protection provisions) and generally fall short of the level of fundamental rights guarantees that are necessary for criminal proceedings. Companies are increasingly expected to facilitate the internal analysis of their fact-finding processes, and adapting e-discovery tools is the most effective way. However, the results of internal e-discovery can only be used as evidence in criminal proceedings without prejudice to the requirement of due process and under conditions of guarantees. The most crucial condition is transparency, i.e. to ensure that the operating mechanism of the e-detection algorithm, based on sophisticated technology, is known to the prosecuting authorities. As there are no generally applicable rules for electronic discovery, the basic assumption is that any such procedure is a "black box".[25] Thus, in order to be able to use the evidence obtained through the use of AI in criminal proceedings, the authorities need to know in advance what the expected outcome of the use of AI will be in a particular case, what technology will be used, what databases will be processed and what monitoring and quality control processes will be in place during the execution of the task. Open and constructive communication between the company and law enforcement authorities is essential, especially regarding the type of algorithm chosen. It should be demonstrated in advance on a narrow database sample project.[26] Thus, an algorithm is not helpful in discovering the substantive, material facts if its

[22] Zs. Fantoly, A. Lichtenstein, *op. cit*.

[23] SIRIUS, *op. cit.*, p. 17.

[24] *Ibidem*.

[25] S.H. Schneider, M. Priewer, *op. cit*.

[26] A. Zachary, R. Chalk, *The Rise of AI in Corporate Investigations*, 6.9.2017, https://www.law360.com/articles/956749?utm_source=LexisNexis&utm_medium=LegalNewsRoom&um_campaign=articles_search (access: 10.12.2024).

operating principles and structure are not transparent to the downstream user bodies and the authorities in charge of criminal matters. In this case, the voluntary acquisition and transfer of evidence in the framework of criminal compliance activities does not add value to the investigation by the authorities and cannot be used as a basis for cooperation. Furthermore, as a fundamental requirement of the rule of law criminal procedure is to ensure a fair trial, this requires, in our case, the emergence of a new type of legal role: a generation of lawyers with a solid knowledge of the technical background of the use of AI and how it works, and who can use this knowledge in their legal arguments in the courtroom.

Transparency is of paramount importance in the criminal justice system in the European Union: "The reliability of information obtained by analyzing large data sets depends on the underlying data, and therefore rigorous scientific and ethical standards are needed to judge the results of the analysis and its predictive algorithms". Furthermore, Member States' law enforcement authorities should be reminded that "data analysis should be applied with the highest ethical standards and ensure human intervention and accountability at all stages of decision-making, not only to assess the representativeness, accuracy, and quality of the data but also to evaluate the appropriateness of each decision to be taken based on that information".[27]

CONCLUSIONS

As early as 1987, Recommendation No. R(87)18 of the Committee of Ministers of the Council of Europe listed several ways of simplifying criminal proceedings, from investigation through prosecution to trial. Generally speaking, the use of AI makes it easier to identify the cases in which it is possible to speed up and simplify criminal proceedings by using such solutions, and also to achieve additional savings in time and costs within the proceedings themselves.

The emergence of AI therefore brings new opportunities for the criminal justice system. Nowadays, criminal compliance activities are becoming increasingly widespread among businesses with economic severe activities, as the development of internal investigation and control methods can be a useful tool both in terms of prevention and cooperation with law enforcement authorities. Data processing using AI makes available a wealth of evidence that would be impossible to collect and assess using traditional law enforcement tools and techniques, primarily relying on human resources. The deployment of AI tools and their operation within an appropriate legal framework truly incentivizes businesses if they can derive tangible benefits from the factual data and information collected and selected by AI during

[27] European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)).

their internal self-disclosure investigations when cooperating with law enforcement authorities. This benefit is nothing less than a significant reduction in the duration of any subsequent criminal sanctions that may be imposed, and the avoidance of prosecution. The cooperation is also worthwhile for the criminal justice authorities, as using AI-based evidence in the context of the company's integral investigation activities is a significant time- and cost-saving factor in criminal proceedings.[28]

REFERENCES

Literature

Ambrus I., Farkas Á., *A compliance alapkérdései. Az etikus vállalati működés elmélete és gyakorlata*, Budapest 2019, **DOI: https://doi.org/10.55413/9789632959344**.

Ambrus I., Mezei K., Molnár E., *Magyarázat a compliance jogszabályairól I. Általános és büntetőjogi compliance*, Budapest 2021.

Herke Cs., *A mesterséges intelligencia kriminalisztikai aspektusai*, "Belügyi Szemle" 2021, vol. 69(10), **DOI: https://doi.org/10.38146/BSZ.2021.10.2**.

Karsai K., *Algorithmic Decisions within the Criminal Justice Ecosystem and Their Problem Matrix*, "International Review of Penal Law / Revue Internationale de Droit Penal" 2021, vol. 92(1).

Knierm T., *Erfordennise und Grenze der Internal Investigation*, [in:] *Wissenschafliche und praktische Aspekte der nationalen und internationalen Compliance-Diskussion*, Baden-Baden 2010.

Molnár E., *A vállalkozáson belüli előnyomozási eljárás interdiszciplináris kontextusban*, "Jogtudományi közlöny" 2016, vol. 71(9).

Momsen C., *Internal Investigations zwischen arbeitsrechtlicher Mitwirkungspflicht und strafprozessualer Selbstbelastungsfreiheit*, "Zeitschrift für Internationale Strafrechtsdogmatik" 2011, vol. 6(6).

Rotsch T., *Criminal Compliance*, Baden-Baden 2015.

Staffer L., Jany O., *Künstliche Intelligenz und Strafrechtsflege – eine Orientierung*, "Zeitschrift für Internationale Strafrechtsdogmatic" 2020, vol. 15(4).

Online sources

Bellapu A., *Artificial Intelligence is Playing a Big Role in Fraud Investigation*, 2.4.2021, https://www.analyticsinsight.net/artificial-intelligence-is-playing-a-big-role-in-fraud-investigation (access: 11.12.2024).

Carrington N., *How Forensic Investigators Gain an Edge with AI*, 22.10.2018, https://www2.deloitte.com/ch/en/pages/forensics/articles/forensic-investigators-gain-an-edge-with-ai.html (access: 11.12.2024).

Casepoint, *How a Multi-Billion Dollar Corporation Reaped Major Cost Savings Conducting an Internal Investigation Using Casepoint*, https://www.casepoint.com/resources/case-studies/corporte-ediscovery-cost-savings-artificial-intelligence (access: 11.12.2024).

Fantoly Zs., Herke Cs., Szabó B., *The Role of AI-based Systems in Negotiated Proceedings*, "e-Revue Internationale de Droit Penal" 2023, vol. 17, https://www.penal.org/de/2023-2 (access: 10.12.2024).

[28] Zs. Fantoly, Cs. Herke, B. Szabó, *op. cit*.

Fantoly Zs., Lichtenstein A., *Siri, Alexa and Co. in the Criminal Justice System: The Use of Virtual Voice Assistants in Criminal Investigation and Their Admissibility as Digital Evidence*, [in:] *Digital Criminal Justice: A Studybook*, Istanbul 2023, https://eta.bibl.u-szeged.hu/5804 (access: 10.12.2024).

Marr B., *The Complete Beginners' Guide to Artificial Intelligence*, 25.4.2017, https://www.forbes.com/sites/bernardmarr/2017/04/25/the-complete-beginners-guide-to-artificial-intelligence/?sh=fda0e364a835 (access: 10.12.2024).

Schneider S.H., Priewer M., *LegalTech: Solutions to Old and New Challenges in Internal Investigations*, 2020, https://www.financierworldwide.com/legaltech-solutions-to-old-and-new-challenges-in-internal-investigations#.Y3DkTnbMI2w (access: 10.12.2024).

SIRIUS, *SIRIUS EU Digital Evidence Situation Report: 2nd Annual Report*, 2020, https://www.eurojust.europa.eu/publication/sirius-eu-digital-evidence-situation-report-2020 (access: 10.12.2024).

Strategic Management Services, *Evaluating Corporate Compliance Programs Using the DOJ "Filip Factors"*, June 2018, https://www.compliance.com/resources/evaluating-corporate-compliance-programs-using-the-doj-filip-factors (access: 11.12.2024).

Zachary A., Chalk R., *The Rise of AI in Corporate Investigations*, 6.9.2017, https://www.law360.com/articles/956749?utm_source=LexisNexis&utm_medium=LegalNewsRoom&um_campaign=articles_search (access: 10.12.2024).

Reports

Committee on Civil Liberties, Justice and Home Affairs, Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)).

Committee on Legal Affairs, Report on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)).

Legal acts

European Parliament resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)).

Recommendation No. R(87)18 of the Committee of Ministers to Member States concerning the simplification of criminal justice of the Council of Europe, adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies.

ABSTRAKT

Państwa szybko sobie uświadomiły, że uproszczenie i przyspieszenie postępowania karnego jest istotne dla podniesienia jego skuteczności. Rozwój systemu kooperacji z organami ścigania oraz związane z nim wprowadzanie nowych narzędzi prawnych to najnowsze osiągnięcia procesów ustawodawczych ostatnich dziesięcioleci. Dotyczy to również rozwiązań *criminal compliance*, które umożliwiają przedsiębiorstwu aktywne uczestnictwo w śledztwie oraz pomoc organowi prowadzącemu czynności. Przedsiębiorstwo uzyskuje pewne korzyści procesowe w zamian za współpracę (np. uniknięcie zarzutów lub istotnie złagodzona kara). Pojawienie się narzędzi sztucznej inteligencji daje nowe możliwości wszystkim instytucjom społeczeństwa, w tym środowisku prawniczemu. W artykule omówiono potencjalne zastosowanie sztucznej inteligencji w kontekście *criminal compliance*.

Słowa kluczowe: *criminal compliance*; sztuczna inteligencja; postępowanie karne