Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 6 (Special Issue)

sciendo

DOI: 10.15290/bsp.2021.26.06.04

Received: 31.07.2021
Accepted: 30.10.2021

Karol Karski
University of Warsaw, Poland
k.karski@wpia.uw.edu.pl
ORCID ID: https://orcid.org/0000–0003-0757–6283

Bartłomiej Oręziak
Cardinal Stefan Wyszyński University in Warsaw, Poland
b.oreziak@uksw.edu.pl
ORCID ID: https://orcid.org/0000–0001-8705–6880

Selected Considerations Regarding the Digitalisation of Criminal Proceedings in Light of the Standards of the Council of Europe: Analysis Taking into Account the Experience of the Current Pandemic

Abstract: The aim of the article is to prepare an analysis in order to formulate propositions regarding the digitalisation of Polish criminal proceedings as regards the administration of justice. These hypotheses would have merited consideration even pre-pandemic, but they demand even more attention as a result of the pandemic. The pandemic has served to highlight the pre-existing necessity to adapt criminal law to the latest observable technical and technological advances. In light of the above, the first issue to be analysed concerns the conditions, procedures, and possibilities surrounding the collection of evidence electronically, taking into account the most recent relevant guidelines of the Council of Europe. The second issue to be examined will be the adaptation of criminal procedures, including Polish, to the standards stipulated in the Convention of the Council of Europe on Cybercrime of 23 November 2001, in light of national norms regarding evidence gathering. The third issue that will be assessed in this study will be the benefits, risks, or potential of the application of artificial intelligence algorithms in criminal procedure. The consideration of each of the three areas will have regard to the present global pandemic. The article concludes with a concise summary containing the authors' conclusions and propositions *de lege ferenda*.
Keywords: artificial intelligence, COVID-19, cyber convention, digitalisation of criminal proceedings, electronic evidence

Introduction

The current SARS-CoV–2 virus pandemic has undoubtedly influenced perceptions of the modern world. The implementation of technological innovations regarding products and processes in many areas of human life has been greatly appreciated. A typical example would be the increasingly common use of digital medical solutions.[1] Although the pandemic is directly associated with issues related to the healthcare sector in its broadest sense, changes in the way specific activities are performed relate or pertain to other issues as well. We can cite the obvious ongoing problems regarding education, for example, where a partial solution to date has been the introduction of remote schooling. Acquiring and conveying knowledge via ICT networks has, of course, both advantages and disadvantages. Nevertheless, it is currently the only feasible method of teaching that can be applied generally. A similar example would be the judiciary where, on the one hand, the negative impact of the SARS-CoV–2 virus can be seen while, on the other, one can see also see the opportunities offered by technical and technological progress. Both positive and negative examples serve to illustrate this point. A positive example would be the growing awareness of the need to digitalise the judiciary. A negative example would concern a change of the examination mode to a remote process with potential procedural delays. This has been confirmed in the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions of 2 December 2020, entitled "Digitalisation of justice in the European Union – A toolbox of Opportunities"[2] which notes,

> "The COVID-19 crisis has thus underlined the need to strengthen the resilience of the justice system across the EU. It has also stressed the further cooperation with its international partners, and promote best practices also in this policy area. This represents an important component of a society based on European values, and of a more resilient economy."[3]

This also applies to criminal proceedings, the issue under analysis, as it is one of the main features of the justice system. It is important that the European

1 See for example: D. Lupton, The digitally engaged patient: Self-monitoring and self-care in the digital health era, "Social Theory & Health" 2013, no. 11(3), p. 257; E. Elenko, L. Underwood, D. Zohar, Defining digital medicine, "Nature biotechnology" 2015, no. 33(5), pp. 456–461; A. André, The Information Technology Revolution in Health Care, (in:) A. André (ed.), Digital Medicine, Cham 2019, p. 4.

2 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 2 December 2020, entitled "Digitalisation of justice in the European Union A toolbox of opportunities" (COM/2020/710 final).

3 *Ibidem*.

institutions address this issue and provide valuable guidelines for the Member States. Similar actions are being undertaken by the Council of Europe. It would be justifiable, therefore, to examine the possibility of putting forward ideas regarding the digitalisation of Polish criminal proceedings that would strengthen the functioning of the justice system by reducing its exposure to risk of disruption by real world events. It is worth re-emphasising that the aim of the analysis in this article is to formulate specific hypotheses regarding the digitalisation of Polish criminal proceedings to strengthen the administration of justice. These ideas would seem justifiable and worthy of consideration both in pandemic-free times and, even more, during the pandemic. In this context, the first issue to be analysed will be the conditions, procedures, and possibilities in general of using electronic evidence in preparatory inquiries. The second issue that will be examined will be the adaptation of the criminal process to meet standards of evidence gathering when fighting cybercrime.[4] The third and final issue to be analysed will be the possibilities of using artificial intelligence algorithms as part of the criminal procedure.[5] The analysis in all three areas will take into consideration the situation caused by the SARS-CoV–2 pandemic and selected standards of the Council of Europe. It will also highlight a specific scientific issue. The three areas indicated above are the principal elements of the digitalisation of the judiciary as selected by the authors. The decisive criterion for the selection of these specific areas of research was the level of their importance for the issue in question and the presence of relevant standards of the Council of Europe. After analysing the entire spectrum of topics that could have been considered, it was decided to pay particular attention to issues related to electronic evidence, cybercrime, and artificial intelligence. Although there are many other possible aspects of the digitalisation of criminal proceedings that could have been included, such as the use of videoconferencing for example, the indicated analytical areas are key examples, in the Authors' opinion, related to the digitalisation of criminal proceedings.

4 See interesting study by: W. Filipkowski, L. Picarella, Criminalizing Cybercrimes: Italian and Polish Experiences, „Białostockie Studia Prawnicze" 2021, no. 26(3), pp. 171–183. Issues related to cybercrime are frequently international. The level of their complexity is similar to matters from the international criminal proceedings area, see generally: E. Karska, Karna jurysdykcja krajowa a międzynarodowa, (in:) J. Kolasa (ed.), Współczesne sądownictwo międzynarodowe, vol. II („Wybrane zagadnienia prawne"), Wrocław 2010, pp. 251–293; E. Socha, Stosunek jurysdykcji Międzynarodowego Trybunału Karnego do sądów krajowych, „Przegląd Czerwonokrzyski" 2002, no. 3–4, pp. 26-27; E. Karska, Międzynarodowe prawo karne, (in:) B. Hołyst, R. Hauser (eds.), Wielka Encyklopedia Prawa, vol. IV: J. Symonides, D. Pyć (eds.), Międzynarodowe prawo publiczne, Warsaw 2014, p. 233.

5 In respect to artificial intelligence please see interesting studies by: A. Maceratini, New Technologies between Law and Ethics: Some Reflections, „Białostockie Studia Prawnicze" 2021, no. 26(3), pp. 9–24; R. Rejmaniak, Bias in Artificial Intelligence Systems, „Białostockie Studia Prawnicze" 2021, no. 26(3), pp. 25–42.

The first of the issues to be analysed is the standardisation of the use of electronic evidence in Polish criminal proceedings. This concerns specifying both procedures and conditions related to the taking of this kind of evidence before a criminal court. This covers not only the provisions of law that decide how the parties shall submit their electronic evidence but also those provisions that specify the rules for assessing the probative value of such evidence and the conditions of their storage by the procedural authorities, which, importantly, should ensure the integrity of the digital data relevant to the subject of the proceedings. In this respect, the "Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings"[6] (hereinafter: the CoE Guidelines) adopted in 2019 by the Committee of Ministers of the Council of Europe and the related secondary document entitled "Explanatory Memorandum of Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings" (hereinafter: the memorandum)[7], provide material guidelines. Both documents were prepared as part of the activity of the European Committee on Legal Cooperation (CDCJ)[8].

After a preamble, the CoE Guidelines contain, on the one hand, a description of the purpose and scope of the regulation, and, on the other, provide definitions and general rules as well as detailed recommendations. This means that the EC Guidelines in fact provide for a number of propositions *de lege ferenda* for the national legislature. At this stage, it is not necessary to cite mechanically the content of these acts but to consider their potential practical application in criminal proceedings.[9] From the outset, as indicated in the title of the CoE Guidelines, the authors have stressed that their intention was to cover only civil and administrative proceedings within the scope of this document. Nevertheless, the content of the provisions of the guidelines

6 Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (CM(2018)169-add1final), https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c (11.10.2021).

7 Explanatory Memorandum of Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (CM(2018)169-add2), https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0e (11.10.2021).

8 European Committee on Legal Cooperation, https://www.coe.int/en/web/cdcj (11.10.2021).

9 In the scope of the practical verification of the changes introduced into criminal proceedings, as noted by P. Hofmański in the context of the Act of 27 September 2013, Amending the Act – Code of Criminal Procedure (Journal of Laws, item 1282): "I am of the opinion that the changes made by the legislator in essence constitute only the beginning of the long road leading to efficient and just criminal proceedings. For most certainly practice must verify the adopted solutions and nobody is able to predict in detail how such verification will progress. Apart from foreseeable results of the amendments, what also remains is the extremely important and unpredictable human factor. It is not fully known how strong the habits of the participants in the proceedings regarding the rules thereof which have remained in force for many years will be" (see: P. Hofmański, Wielka reforma Kodeksu postępowania karnego 2013, "Forum Prawnicze" 2013, no. 18(4), p. 10).

contained in the CoE Guidelines is extremely open in nature and not focused on the specific nature of either civil or administrative proceedings. In support of this thesis, one may cite the wording of the general principles of the CoE Guidelines,

> "It is for courts to decide on the potential probative value of electronic evidence in accordance with national law. Electronic evidence should be evaluated in the same way as other types of evidence, in particular regarding its admissibility, authenticity, accuracy, and integrity. The treatment of electronic evidence should not be disadvantageous to the parties or give unfair advantage to one of them"[10],

One of the subsequent detailed recommendations states,

> "Transmission of electronic evidence by electronic means should be encouraged and facilitated in order to improve efficiency in court proceedings."[11]

This presupposes that the CoE Guidelines may also be successfully applied in criminal proceedings, since their application constitutes "good advice" that would benefit the electronic justice system. Incidentally, it may also be emphasised that such a theoretical as well as practical possibility of using the CoE Guidelines generally in any judicial proceedings in which electronic evidence is submitted.[12] This depends entirely on the will of the national legislator which may decide that the CoE Guidelines should be applied to a broader extent than that implied by the title.[13]

Taking into account the current pandemic situation caused by the SARS-CoV–2 virus, the application of the CoE Guidelines may bring real benefits to criminal proceedings. In light of the increased number of criminal proceedings in which digital evidence is used as an inevitable result of the restrictions stemming from the pandemic, it appears necessary to resort to procedures and conditions related to the taking of this kind of evidence before criminal courts. The CoE Guidelines can and should serve in this regard as valuable guidance as to how a procedural authority is to deal with electronic evidence. It seems that the biggest benefit that the CoE Guidelines can bring to criminal proceedings in the context of electronic evidence is to support the effective and accurate fact finding for a particular case.

10 Guidelines of the Committee of Ministers of the Council of Europe…

11 *Ibidem*.

12 In criminal proceedings in Poland the possibility to take evidence follows from the absence of the so-called formal theory of evidence (K. Boratyńska, M. Królikowski, Komentarz do art. 167, (in:) A. Sakowicz (ed.), Kodeks postępowania karnego. Komentarz, Warsaw 2016, p. 429). Additionally, following legal literature, it may also be stated than in Polish criminal proceedings there exists the possibility to take any evidence of material value for the resolution of the case (R. Kmiecik, Dowód ścisły w procesie karnym, Lublin 1983, p. 46).

13 It should be remembered that the CE Guidelines are a typical example of so-called soft law.

This undoubtedly leads to the realisation of the value of truth[14]in criminal procedural law as a basic goal of criminal proceedings, and thus to its fulfilment. For all of these reasons, consideration by the legislator of the application of the CoE Guidelines in the area of criminal procedure is highly recommended *de lege ferenda*. It should be noted that the impact of the CoE Guidelines in this way belongs to the field of so-called soft law.

1. The Convention on Cybercrime in Criminal Proceedings

The second point for consideration is the necessity to adapt Polish criminal proceedings to the standards set out in the Council of Europe Convention on Cybercrime signed in Budapest on 23 November 2001 (hereinafter: Budapest Convention).[15]It is an indisputable fact that the Budapest Convention, as an international treaty, is binding on the states that have ratified and acceded to it. Thus, by ratifying the Budapest Convention on 20 February 2015, Poland decided to accept an international legal obligation to adapt its normative order to the standards of this international agreement. The agreement entered into force for Poland on 1 June 2015.[16]

14 M. Wielec, Wartości – Analiza z perspektywy osobliwości postępowania karnego, Lublin 2017, pp. 149–277; S. Judycki, O klasycznym pojęciu prawdy, „Roczniki Filozoficzne" 2001, no. 49, pp. 25–26; J. Jackson, Two methods of proof in criminal procedure, „The Modern Law Review" 1988, no. 51(5), p. 554; S. Judycki, Prawda i kryterium prawdy: korespondencja, koherencja, praktyka, „Kwartalnik Filozoficzny" 1999, no. 28, pp. 23–45; J. Zajadło, Teoretyczne i filozoficzno-prawne pojęcie prawdy, (in:) K. Kremens, J. Skorupka (ed.), Pojęcie, miejsce i znaczenie prawdy w procesie karnym, Wrocław 2013, pp. 20–32; S. Waltoś, Zasada prawdy materialnej, (in:) P. Wiliński (ed.), System Prawa Karnego Procesowego, Warsaw 2014, pp. 273–281; J. Jodłowski, Zasada prawdy materialnej w postępowaniu karnym. Analiza w perspektywie funkcji prawa karnego, Warsaw 2015, pp. 54–71; J. Dębowski, O klasycznej koncepcji prawdy i jej filozoficznych podstawach. Czy w Matrixie możliwa jest prawda?, (in:) A. Kiklewicz, E.Starzyńska-Kościuszko (eds.), Oblicza prawdy w filozofii, kulturze, języku, Olsztyn 2014, pp. 12–15; M. Strogowicz, Prawda obiektywna i dowody sądowe w radzieckim procesie karnym, Warsaw 1959, p. 85; A. Murzynowski, Istota i zasady procesu karnego, Warsaw 1976, p. 131; J. Jabłońska-Bonca, O prawie, prawdzie i przekonywaniu, Koszalin 1999, p. 80; M. Klejnowska, C. Kłak, Z. Sobolewski, Proces karny. Część ogólna, Warsaw 2011, p. 45.

15 The Convention of the Council of Europe on Cybercrime signed in Budapest on 23 November 2001 (Journal of Laws of 2015, item 728; ETS No.185); See: J. Clough, A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonization, "Monash University Law Review" 2014, no. 40(3), pp. 698–736; M. Gercke, The Convention on Cybercrime, "Multimedia und Recht" 2004, no. 20, p. 802.

16 The government's declaration of 2 April 2015, on the binding force of the Convention on Cybercrime of the Council of Europe signed in Budapest on 23 November 2001 (Journal of Laws, item729); Council of Europe, 'Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime: Status as of 09/06/2021', https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=E7ydoPfD (11.10.2021).

Irrespective of internal constitutional regulations, this is confirmed by the commonly understood international custom, pursuant to which treaties are to be observed and performed in good faith (*pacta sunt servanda*)[17]. The intention is to adapt the legal systems of the States Parties, as the Budapest Convention is not of a self-executing nature.[18] Its individual provisions begin with the words: "Each Party shall adopt such legislative and other measures as may be necessary to ensure (…)." This is of fundamental importance in determining how to implement its standards through national law. For example, Articles 2 to 9 of the Budapest Convention make proposals regarding the classification of types of cybercrime in the form of offences relating to confidentiality, integrity, and access to IT data and systems (illegal access, illegal interception of data, data interference, system interference, and misuse of devices), computer-related offences (computer-related forgery and computer-related fraud), offences related to the nature of the possessed data (child pornography) and offences related to infringements of copyright and related rights.

In order to fulfil the international obligations arising from these provisions of the Budapest Convention, each State Party should introduce the appropriate provisions into its legal system. In Polish law, relevant legal measures to incorporate the Budapest Convention include, *inter alia*, Articles 267, 268, 268a and 269b of the Criminal Code.[19] This means that, without an act to incorporate the provisions of the Budapest Convention into the national legal order, they remain ineffective and cannot be directly invoked. Precisely the same situation occurs in the case of the procedural norms of the Budapest Convention, where the States Parties are obliged to adopt measures relating to the collection of evidence such as the expedited preservation of stored computer data (expeditious preservation of stored computer data and the preservation and partial disclosure of traffic data), and relating to orders to deliver, search, and seize stored computer data and to collect computer data in real time (real-time collection of traffic data and the interception of content data).

The indicated measures relating to evidence used in combatting cybercrime should be regarded as the appropriate standards of the Council of Europe in this respect. Their incorporation into the Polish legal system is guaranteed by the provisions

17 P. Grez, Pacta sunt servanda, "Revista Actualidad Juridica" 2008, no. 18, pp. 107–187; M. Shaw, International Law, Leicester 2008, pp. 86–89.

18 On the subject of self-executing and non-self-executing international treaties see.: J. Paust, Self-executing treaties, "The American Journal of International Law" 1988, no. 82(4), pp. 760–783; C. Bradley, Intent, Presumptions, and Non-Self-Executing Treaties, "The American Journal of International Law" 2008, no. 102(3), pp. 540–551. On the subject of practical examples of implementing international obligations into Polish criminal law see, for example, E. Socha, Zakres włączenia katalogu zbrodni objętych jurysdykcją Międzynarodowego Trybunału Karnego do polskiego prawa karnego materialnego, "Przegląd Sejmowy" 2007, vol. XV, no. 5(82), pp. 253–266.

19 Act of 6 June 1997 – The Criminal Code (consolidated text: Journal of Laws of 2020, item 1444, as amended).

of Articles 218a and 236a of the Code of Criminal Procedure,[20] which provide for the use of modern technologies in the course of the collection of evidence.[21] Nevertheless it may seem that the resulting normative content may be insufficient, which leaves certain doubts as to the full implementation of the standards of the Council of Europe in this regard into the Polish legal system. To put it more precisely, we are talking about the introduction of the appropriate measures in national law, which facilitate the possibility of applying the rules relating to evidence provided for in the Budapest Convention in the operating practice of the law enforcement authorities.

Without prejudging at this point whether or not the legal international obligations in this respect have been fulfilled by Poland, as this issue requires a separate analysis as has already been indicated above, doubts of this kind may give rise to the impossibility on the part of the competent authorities to use fully the instruments indicated above to combat cybercrime, because, as has been stressed, it is not self-executing. For this reason, it is worth postulating *de lege ferenda* that the full incorporation of the criminal and procedural standards set out in the Budapest Convention into the Code of Criminal Procedure, every standard of the CoE Guidelines will have its counterpart in national law. Only in this way is it possible to guarantee that Polish law enforcement authorities have unquestionable legal grounds to collect evidence as provided for in the Budapest Convention. Given the specificity of cybercrime, its transnational nature, it is also of key importance for international cooperation in the field of combatting cybercrime.[22] Although this hypothesis remains warranted regardless of the epidemic conditions prevailing in the country, it is reinforced by the current situation caused by the COVID-19 pandemic, giving rise to a significant increase of criminal activity on the Internet. In this era of health-driven digitalisation of everyday activities, it becomes even more necessary and important to equip the competent law enforcement authorities that protect the security of Internet users

20 Act of 6 June 1997 – The Code of Criminal Procedure (consolidated text: Journal of Laws of 2021, item 534).

21 Pursuant to Article 218a. § 1 of the Code of Criminal Procedure, government offices, institutions, and entities operating in the telecommunications sector are obliged to promptly secure, upon the demand of a court or public prosecutor contained in the order, for a specified period of time, which shall not however exceed 90 days, computer data stored in devices containing the data, on a data carrier or in the computer system. The provision of Article 218 § 2 second sentence shall apply accordingly. In turn, pursuant to Article 236a of the Code of Criminal Procedure, the provisions of chapter 25 ("Seizure of objects and searches") apply accordingly to the person who is the holder and user of a device containing computer data or computer system, with regard to computer data stored in that device or system or a carrier in that person's disposal or used thereby, including in correspondence sent by e-mail.

22 It is worth mentioning the ongoing negotiations of the second additional protocol to the Budapest Convention, in particular with regard to the draft provisions on cooperation with private partners, https://www.coe.int/en/web/cybercrime/t-cy-drafting-group (11.10.2021).

with appropriate legal instruments to combat cybersecurity.[23] It should be stressed that the hypothesis raised above falls within the scope of hard law.

2. Artificial Intelligence in Criminal Proceedings

The third issue for consideration is the possibility of using artificial intelligence algorithms in Polish criminal procedure. It should be emphasised, however, that this proposition is not intended to dehumanise the judiciary, but rather to support it through the use of the opportunities offered by the use of modern technology of this kind.[24] These possibilities are as diverse as the scope of the concept of artificial intelligence is broad. The literature emphasises that "AI refers to the

23 Regarding the correlation between criminal proceedings and modern technologies, see: S. Brenner, J. Schwerha, Introduction-Cybercrime: A Note on International Issues, "Information Systems Frontiers" 2004, no. 6(2), pp. 111–114; S. Moitra, Developing Policies for Cybercrime, "European Journal of Crime, Criminal Law and Criminal Justice" 2005, no. 13(3), pp. 435–464; M. Nuth, Taking Advantage of New Technologies: For and Against Crime Computer Law and Security Report, "Computer Law & Security Review" 2008, no. 24, pp. 437–446; N. Katyal, Criminal Law in Cyberspace, "University of Pennsylvania Law Review" 2001, no. 149(4), pp. 1003–1114; C. Coleman, Security Cyberspace – New Laws and Developing Strategies, "Computer Law and Security Report" 2003, no. 19(2), pp. 131–136; R. Winick, Searches and seizures of computers and computer data, "Harvard Journal of Law & Technology" 1994, no. 8(1), pp. 75–128; L. Lessig, P. Resnick, Zoning Speech on the Internet: A Legal and Technical Model, "Michigan Law Review" 1999, no. 98(2), pp. 395–431; L. Speer, Redefining Borders: The Challenges of Cybercrime, "Crime, Law and Social Change" 2000, no. 34, pp. 259–273; J. Reidenberg, Technology and Internet Jurisdiction, "University of Pennsylvania Law Review" 2005, no. 153(6), pp. 1951–1974; B. Boni, Creating a Global Consensus Against Cybercrime, "Network Security" 2001, no. 9, pp. 18–19; D. Resseguie, Computer Searches and Seizure, "Cleveland State Law Review" 2000, no. 48(185), pp. 185–214; N. Marion, Symbolic Policies in Clinton's Crime Control Agenda, "Buffalo Criminal Law Review" 1997, no. 1, pp. 67–108; P. Swire, Elephants and Mice Revisited: Law and Choice of Law on the Internet, "University of Pennsylvania Law Review" 2005, no. 153(6), pp. 1975–2001; A. Shapiro, The Internet, "Foreign Policy" 1999, no. 115, pp. 14–27; A. Stolz, Congress and Capital Punishment: An Exercise in Symbolic Politics, "Law and Policy Quarterly" 1983, no. 5(2), pp. 157–180.

24 As regards the possibility and justifiability of according legal personality to artificial intelligence: A. Silverman, Mind, Machine, and Metaphor. An Essay on Artificial Intelligence and Legal Reasoning. Boulder, Colorado 1993, p. 1; K. Bowrey, Ethical Boundaries and Internet Cultures, (in:) L. Bently, S. Maniatis (eds.), Intellectual Property and Ethics, London 1998, p. 36; D. Partridge, A New Guide to Artificial Intelligence, New Jersey 1991, p. 1. See also: M. Jankowska, Podmiotowość prawna sztucznej inteligencji?, (in:) A. Bielska-Brodziak (ed.), O czym mówią prawnicy mówiąc o podmiotowości, Katowice 2015, pp. 171–197; J. Byrski, Oprogramowanie zawierające elementy sztucznej inteligencji. Wybrane zagadnienia prawne, (in:) P. Kostański, P. Podrecki, T. Targosz (eds.), Experientia Docet. Księga jubileuszowa ofiarowana Pani Profesor Elżbiecie Traple, Warsaw 2017, pp. 1331–1343; V. P. Talimonchik, The Prospects for the Recognition of the International Legal Personality of Artificial Intelligence, "Laws" 2021, no. 10(4)(85), pp. 1-11.

branch of computer science dedicated to the development of computer algorithms to accomplish tasks traditionally associated with human intelligence, such as the ability to learn and solve problems."[25] For this reason, it is frequently stressed that AI is a family of technologies and scientific fields that allows for greater automation, acceleration, and repeatability of human perception, decision-making, and reasoning.[26] In addition, it is important to divide AI into two models of application. We refer here to the classical model and the connectionist model.[27] In the former, AI operates on the basis of a database that has been created at the programming stage and performs strictly defined tasks, whereas in the latter case AI operates on the basis of neural networks, independently acquiring data and demonstrating self-learning features.[28]

This means that the possibilities of using AI in criminal proceedings are extremely wide.[29] Using the connectionist model of AI, it would be possible for it to perform all of the activities of a judicial authority independently, with or without human supervision. Technological progress in the 21st century makes it possible to adopt different variations of the use of AI in criminal proceedings. At this point, a regulatory approach is recommended in the law that, without hampering the development of this type of technology, will enable it to be controlled and used by state authorities. In this context, a relevant standard is the document entitled "European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment" (hereinafter: the European AI Ethical Charter) adopted by the Council of Europe on 3–4 December 2018, at the 31st plenary session of the European Commission for the Efficiency of Justice.[30] This document is based on five basic principles to be respected when using AI in judicial systems. They indicate such issues as respect for fundamental rights, respect for the principle of non-discrimination, adherence to the concept of "under user control," and the necessity to ensure quality, security, transparency, impartiality, and fairness when using of AI. These principles are valuable guidelines for the national legislator, and are sensitive to the currently perceptible process of technical, technological, or

25 A. Tang, R. Tam, A. Cadrin-Cheenevert, W. Guest, J. Chong, J. Barfett, L. Chepelev, R. Cairns, J. Ross, M. Cicero, M. Poudrette, J. Jaremko, C. Reinhold, B. Gallix, B. Gray, R. Geis, Canadian Association of Radiologists White Paper on Artificial Intelligence in Radiology, "Canadian Association of Radiologists Journal" no. 69(2), p. 122.

26 A. Renda, Artificial Intelligence. Ethics, governance and policy challenges. Report of a CEPS Task Force, Brussels 2019, pp. 7–27.

27 A. Chłopecki, Sztuczna inteligencja – szkice prawnicze i futurologiczne, Warsaw 2018, p. 5.

28 M. Jankowska, Podmiotowość…, *op. cit.*, pp. 171–197.

29 In this context, it should be mentioned that the European Commission issued a "Proposal for a Regulation laying down harmonised rules on artificial intelligence" (COM/2021/206 final).

30 European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c (11.10.2021).

civilizational progress, accompanied by an increasing use of artificial intelligence in modern technology in practical applications. In light of the above, it is proposed *de lege ferenda* that the indicated standard of the Council of Europe be taken into account in the Polish normative system. We are referring here to the use of AI algorithms in Polish criminal proceedings, which operate on the basis of a search or analytical engine. AI algorithms of this kind, as it has already been stressed, do not dehumanise the judiciary, but seek to support the work of those performing their duties in this area through automation, acceleration, and repeatability of human perception. A good example would concern programmes to analyse extensive case files, which might demonstrate numerous relationships between the factual circumstances that were, at first glance, unnoticeable. It seems that the careful implementation of the solution under analysis at this point, in line with the principles set out in the European AI Ethical Charter, could, in principle, bring considerable benefits. One of the unquestioned benefits is increasing the independence of the functioning of the judiciary from the conditions of the outside world. It is also worth pointing out that the introduction of the above solutions to the Polish normative order would facilitate the efficiency of trials, thus contributing to the reduction of the phenomenon of excessively long proceedings, and thus positively improving the shape of the legal order which, to a high degree, still embodies the principle of the rule of law

The current epidemiological situation caused by the SARS-CoV–2 virus has emphasised the necessity to ensure the continuity of the functioning of the criminal justice system. In this respect, the judiciary may be compared the state's critical infrastructure. The pandemic has shown how the medical situation can affect the state's ability to organise court proceedings, and thus the pursuit by citizens of their rights and freedoms. This is a situation that must be considered unsatisfactory. The implementation of innovative solutions into the justice system, including criminal proceedings, which would make it more resistant to the negative consequences of conditions arising beyond the scope of its activity, should be postulated. It would seem that one such solution is the use of AI algorithms that would perform data searches or analyses of the state of facts and law. It should be emphasised that this observation applies not only in times of pandemic. It may, however, be particularly beneficial during the ongoing pandemic to implement certain changes in criminal proceedings such as, for example, remote hearings or remote examinations, *i.e.*, solutions enabling the performance of procedural activities without the need for attendance in person. This would greatly facilitate and accelerate the work of the procedural authorities in complex cases, in particular cybercrime cases. This means that *de lege ferenda,* these solutions would work best in the evidence collection process in Polish criminal procedure. Finally, it should be noted that the proposition above is another example of soft law.

Conclusions

In summarising the presented selected propositions regarding the digitalisation of criminal proceedings in light of the standards of the Council of Europe and the present pandemic situation, it should be noted that putting them forward for consideration would also have been warranted in non-pandemic times. The pandemic has only accentuated the need for their implementation into Polish criminal proceedings. In other words, these times have shown what the consequences may be of failing to adapt formal criminal law to the realities of technical, technological, or civilizational progress that are apparent today. Based on the arguments presented here, outlining specific scientific problems, it is highly recommended *de lege ferenda* that the Polish legislator undertakes three steps. The first is to consider the possibility of applying the CoE Guidelines within the framework of the Polish criminal procedure. This will support the effective and factual determination of the reality of a given case, in order to establish the truth, and thus to fulfil the purpose of the criminal procedure. The second is the incorporation of criminal and procedural standards set out in the Budapest Convention into the Code of Criminal Procedure, where each CoE standard will have its equivalent in national law. This will guarantee that Polish law enforcement authorities have an unquestionable legal basis to conduct the collection of evidence as provided for in the Budapest Convention, which also has a direct impact on international cooperation in combatting cybercrime. The third is the use of AI algorithms in Polish criminal proceedings, taking into account the provisions of the European AI Ethical Charter. Firstly, it is recommended to use AI solutions in search or analytical engines. Through automation, acceleration, and repeatability of human perception, this will considerably facilitate and expedite the work of the procedural authorities in complex cases, in particular cases concerning cybercrime. In this respect the decision to reactivate in 2021 the Working Group for Artificial Intelligence, operating at the Office of the President of the Council of Ministers, is an interesting initiative. Finally, it should be emphasised that all of the propositions presented regarding the digitalisation of Polish criminal proceedings in light of the standards of the Council of Europe were also valid and justified prior to the pandemic caused by the SARS-CoV–2 virus. In its turn, the pandemic has shown how much the introduction of these concepts into the normative system is required when facing extraordinary circumstances. It is, however, necessary to verify their usefulness in practice.

REFERENCES

André A., The Information Technology Revolution in Health Centre, (in :) A. André (ed.), Digital Medicine, Cham 2019.

Boni B., Creating a Global Consensus Against Cybercrime, "Network Security" 2001, no. 9.

Boratyńska K., M. Królikowski, Komentarz do art. 167, (in) A. Sakowicz (ed.), Kodeks postępowania karnego. Komentarz, Warszawa 2016.

Bowrey K., Ethical Boundaries and Internet Cultures, (in:) L. Bently, S. Maniatis (eds.), Intellectual Property and Ethics, London 1998.

Bradley C., Intent, Presumptions, and Non-Self-Executing Treaties, "The American Journal of International Law" 2008, no. 102(3).

Brenner S., Schwerha J., Introduction-Cybercrime: A Note on International Issues, "Information Systems Frontiers" 2004, no. 6(2).

Byrski J., Oprogramowanie zawierające elementy sztucznej inteligencji. Wybrane zagadnienia prawne, (in:) P. Kostański, P. Podrecki, T. Targosz (eds.), Experientia Docet. Księga jubileuszowa ofiarowana Pani Profesor Elżbiecie Traple, Warszawa 2017.

Chłopecki A., Sztuczna inteligencja – szkice prawnicze i futurologiczne, Warszawa 2018.

Clough J., A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonization, "Monash University Law Review" 2014, no. 40(3).

Coleman C., Security Cyberspace – New Laws and Developing Strategies, "Computer Law and Security Report" 2003, no. 19(2).

Dębowski J., O klasycznej koncepcji prawdy i jej filozoficznych podstawach. Czy w Matrixie możliwa jest prawda?, (in:) A. Kiklewicz, E. Starzyńska-Kościuszko (eds.), Oblicza prawdy w filozofii, kulturze, języku, Olsztyn 2014.

Elenko E., L. Underwood, D. Zohar, Defining digital medicine, "Nature biotechnology" 2015, no. 33(5).

Filipkowski W., L. Picarella, Criminalizing Cybercrimes: Italian and Polish Experiences, „Białostockie Studia Prawnicze" 2021, no. 26(3).

Gercke M., The Convention on Cybercrime, "Multimedia und Recht" 2004, no. 20.

Grez P., Pacta sunt servanda, "Revista Actualidad Juridica" 2008, no. 18.

Hofmański P., Wielka reforma Kodeksu postępowania karnego 2013, "Forum Prawnicze" 2013, no. 4(8).

Jabłońska-Bonca J., O prawie, prawdzie i przekonywaniu, Koszalin 1999.

Jackson J., Two methods of proof in criminal procedure, "The Modern Law Review" 1988, no. 51(5).

Jankowska M., Podmiotowość prawna sztucznej inteligencji?, (in:) A. Bielska-Brodziak (ed.), O czym mówią prawnicy mówiąc o podmiotowości, Katowice 2015.

Jodłowski J., Zasada prawdy materialnej w postępowaniu karnym. Analiza w perspektywie funkcji prawa karnego, Warszawa 2015.

Judycki S., O klasycznym pojęciu prawdy, "Roczniki Filozoficzne" 2001, no. 49.

Judycki S., Prawda i kryterium prawdy: korespondencja, koherencja, praktyka, "Kwartalnik Filozoficzny" 1999, no. 28.

Karska E., Karna jurysdykcja krajowa a międzynarodowa, (in:) J. Kolasa (ed.), Współczesne sądownictwo międzynarodowe, Vol. II („Wybrane zagadnienia prawne"), Wrocław 2010.

Karska E., Międzynarodowe prawo karne, (in:) B. Hołyst, R. Hauser (eds.), Wielka Encyklopedia Prawa, vol. IV: J. Symonides, D. Pyć (eds.), Międzynarodowe prawo publiczne, Warszawa 2014.

Katyal N., Criminal Law in Cyberspace, "University of Pennsylvania Law Review" 2001, no. 149(4).

Klejnowska M., Kłak C., Sobolewski Z., Proces karny. Część ogólna, Warszawa 2011.

Kmiecik R., Dowód ścisły w procesie karnym, Lublin 1983.

Lessig L., Resnick P., Zoning Speech on the Internet: A Legal and Technical Model, "Michigan Law Review" 1999, no. 98(2).

Lupton D., The digitally engaged patient: Self-monitoring and self-care in the digital health era, "Social Theory & Health" 2013, no. 11(3).

Maceratini A., New Technologies between Law and Ethics: Some Reflections, „Białostockie Studia Prawnicze" 2021, no. 26(3).

Marion N., Symbolic Policies in Clinton's Crime Control Agenda, "Buffalo Criminal Law Review" 1997, no. 1.

Moitra S., Developing Policies for Cybercrime, "European Journal of Crime, Criminal Law and Criminal Justice" 2005, no. 3(3).

Murzynowski A., Istota i zasady procesu karnego, Warszawa 1976.

Nuth M., Taking Advantage of New Technologies: For and Against Crime Computer Law and Security Report, "Computer Law & Security Review" 2008, no. 24.

Partridge D., A New Guide to Artificial Intelligence, New Jersey 1991.

Paust J., Self-executing treaties, "The American Journal of International Law" 1988, no. 82(4).

Reidenberg J., Technology and Internet Jurisdiction, "University of Pennsylvania Law Review" 2005, no. 153(6).

Rejmaniak R., Bias in Artificial Intelligence Systems, „Białostockie Studia Prawnicze" 2021, no. 26(3).

Renda A., Artificial Intelligence. Ethics, governance and policy challenges. Report of a CEPS Task Force, Brussels 2019.

Resseguie D., Computer Searches and Seizure, "Cleveland State Law Review" 2000, no. 48(185).

Shapiro A., The Internet, "Foreign Policy" 1999, no. 115.

Shaw M., International Law, Leicester 2008.

Silverman A., Mind, Machine, and Metaphor. An Essay on Artificial Intelligence and Legal Reasoning. Boulder, Colorado 1993.

Socha E., Zakres włączenia katalogu zbrodni objętych jurysdykcją Międzynarodowego Trybunału Karnego do polskiego prawa karnego materialnego, "Przegląd Sejmowy" 2007, vol. XV, no. 5(82).

Socha E., Stosunek jurysdykcji Międzynarodowego Trybunału Karnego do sądów krajowych, „Przegląd Czerwonokrzyski" 2002, no. 3–4.

Speer L., Redefining Borders: The Challenges of Cybercrime, "Crime, Law and Social Change" 2000, no. 34.

Stolz A., Congress and Capital Punishment: An Exercise in Symbolic Politics, "Law and Policy Quarterly" 1983, no. 5(2).

Strogowicz M., Prawda obiektywna i dowody sądowe w radzieckim procesie karnym, Warszawa 1959.

Swire P., Elephants and Mice Revisited: Law and Choice of Law on the Internet, "University of Pennsylvania Law Review" 2005, no. 153(6).

Talimonchik V. P., The Prospects for the Recognition of the International Legal Personality of Artificial Intelligence, "Laws" 2021, no. 10(4)(85).

Tang A., Tam A., Cadrin-Cheenevert B., Guest W., Chong J., Barfett J., Chepelev L., Cairns R., Ross J., Cicero M., Poudrette M., Jaremko J., Reinhold C., Gallix B., Gray B., Geis R., Canadian Association of Radiologists White Paper on Artificial Intelligence in Radiology, "Canadian Association of Radiologists Journal" no. 69(2).

Waltoś S., Zasada prawdy materialnej, (in:) P. Wiliński (ed.), System Prawa Karnego Procesowego, Warszawa 2014.

Wielec M., Wartości – Analiza z perspektywy osobliwości postępowania karnego, Lublin 2017.

Winick R., Searches and seizures of computers and computer data, "Harvard Journal of Law & Technology" 1994, no. 8(1).

Zajadło J., Teoretyczne i filozoficzno-prawne pojęcie prawdy, (in:) K. Kremens, J. Skorupka (eds.), Pojęcie, miejsce i znaczenie prawdy w procesie karnym, Wrocław 2013.