UNIVERSITY OF BIALYSTOK
FACULTY OF LAW

BIALYSTOK LEGAL STUDIES

BIAŁOSTOCKIE STUDIA PRAWNICZE

BIAŁYSTOK 2021 VOLUME 26 nr 3

BIALYSTOK LEGAL STUDIES

BIAŁOSTOCKIE STUDIA PRAWNICZE

VOLUME 26 nr 3

The original version of the journal is a print one.

ISSN 1689–7404
e-ISSN 2719–9452

Volume Theme Editors: Rafał Rejmaniak, Maciej Aleksandrowicz, Marta Andruszkiewicz
Language Editors: Urszula Andrejewicz, Claire Taylor Jay
Statistical Editor: Ewa Glińska
Graphic and Typographic Development: Jerzy Banasiuk
Cover Design: Bogusława Guenther
Publisher: Faculty of Law, University of Białystok; Temida 2
All volumes can be purchased from Wydawnictwo Temida 2. Address: ul. A. Mickiewicza 1, 15-213 Białystok, Poland. E-mail: temida2@uwb.edu.pl, Tel. +48 85 745 71 68

Contents

Contents

ARTICLES

Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.01

Received: 10.12.2020
Accepted: 30.03.2021

Arianna Maceratini
University of Macerata, Italy
arianna.maceratini@unimc.it
ORCID ID: https://orcid.org/0000-0001-7519-9016

New Technologies between Law and Ethics: Some Reflections

Abstract: This article proposes a reflection on the relationship between ethics, law and new technologies. The relevance of the debate is testified by numerous initiatives and measures, both European and international, which aim to offer answers, necessarily not definitive but evolving, to phenomena such as the development of the internet of things, the incessant extraction and use of big data and, more generally, advances in artificial intelligence and robotics. From this perspective, issues such as respect for privacy and human dignity are raised, to be balanced with the right to inform and be informed as a sign of an effectively shared knowledge. What emerges is the need for a deep critical consideration of the guarantee of individual and collective spheres of action, removed from the domination of market interests, in the affirmation of prevailing and non-negotiable rights. Equally indispensable is the critical attention given to the limits to be placed on human manipulation and alteration, and on the relationship between human being and machine. This assumes a particular ethical, legal and prescriptive meaning aimed at guaranteeing the pluralism of values and dialogue typical of every democratic society.
Keywords: artificial intelligence, knowledge, new technologies, privacy, roboethics

Introductory notes

The increasingly pervasive intelligence of data focuses reflection on the relationship between ethics and law, shifting the centre of the discussion from what is legal to what is morally acceptable. The relevance of this debate is shown by numerous initiatives,[1] and these issues have been significantly highlighted by the

1 We can remember, among others, the 40th International Conference of Authorities for the Protection of Personal Data (ICDPPC) on 'Debating Ethics: Respect and Dignity in Data-Driven Life', held in Brussels from 22 to 26 October 2018 and having as its theme ethics linked to digital

Covid-19 pandemic,[2] which has highlighted the need for effective balancing between state-mandated restrictions and individual autonomy. After all, the centrality of human beings and the guarantee of their dignity represent the direction indicated by the European Community, ensuring an adequate ethical and legal framework as well as demonstrating the two resolutions of the European Parliament, *Civil Law Rules on Robotics* and *A Comprehensive European Industrial Policy on Artificial Intelligence and Robotics*,[3] by the many communications of the Commission on this issue and, not least, by the guidelines of the independent group of 52 experts set up by the Commission in 2018, the High-Level Expert Group on Artificial Intelligence.[4] Significantly, however, in the current state of European Union law, there is no consolidated definition of artificial intelligence capable of defining a phenomenon that increasingly requires new and different regulatory responses to those already in force, which crosses ethical and legal rules that will be applied, just like artificial intelligence, to the most diverse fields of human experience, and which overcomes the classic distinction between public and private in many respects.[5]

In this debate, the right to privacy seems to emerge as a prerequisite for the exercise of any other fundamental rights, as affirmed by the UN Declaration of Human Rights, by the International Covenant on Civil and Political Rights and in many other international and regional treaties, such as in states' constitutions.[6]

development. This assembly provided for the establishment of a permanent working group on ethics and the protection of personal data in artificial intelligence contexts. These issues were taken up and deepened by the 41st International Conference of Authorities for the Protection of Personal Data on 'Convergence and Connectivity Raising Global Data Protection Standards in the Digital Age', which was held in Tirana (Albania) from 21 to 24 October 2019.

2 On ECtHR judgments concerning the right of a patient to have his or her privacy respected, and the corresponding duty of doctors to keep medical confidentiality, see A. Wnukiewicz-Kozłowska, The Right to Privacy and Medical Confidentiality – Some Remarks in Light of ECtHR Case Law, "Białostockie Studia Prawnicze" 2020, vol. 25, no. 2, pp. 185–197.

3 Resolution of the European Parliament of 16 February 2017, Civil Law Rules on Robotics, https://www.europarl. europa.eu/doceo/document/TA-8-2017-0051_EN.html?redirect (accessed 19.10.2020); Resolution of the European Parliament of 12 February 2019, A Comprehensive European Industrial Policy on Artificial Intelligence and Robotics, https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html (accessed 19.10.2020). On the relationship between fundamental rights and artificial intelligence in the approach of the European Union, see M. Zanichelli, Affidabilità, diritti fondamentali, centralità dell'essere umano: una strategia europea per l'intelligenza artificiale, 'i-lex' 2019, vol. 12, pp. 1–23, http://www.i-lex.it/articles/volume12/fascicolo1-3/zanichelli.pdf (accessed 19.10.2020).

4 AI HLEG, https://ec.europa.eu/digital-single-market/en/artificial-intelligence (accessed 08.10.2020).

5 A. Longo and G. Scorza, Intelligenza artificiale. L'impatto sulle nostre vite, diritti e libertà, Milan 2020, pp. 194–195.

6 Universal Declaration of Human Rights, https://www.ohchr.org/en/udhr/documents/udhr_translations/eng.pdf (accessed 09.11.2020); International Covenant on Civil and Political Rights, https://www.ohchr.org/Documents/ Professionalinterest/ccpr.pdf (accessed 09.11.2020).

Equally essential is a dialectical reflection on the possible developments of artificial intelligence and the necessary respect for ethical principles in the legal framework of modern and pluralist democracies.

1. Knowledge and Privacy

In the *new economy*,[7] the possibility of collecting, processing and comparing personal information leads to a redefinition of individual self-determination capable of placing knowledge and the effectiveness of its guarantee at the centre of attention. In this line of reflection, also indicated by Opinion 8/2014 *On the Recent Development on the Internet of Things* of the Article 29 Data Protection Working Party (WP29) (replaced in 2018 by the European Data Protection Board (EDPB) under the EU General Data Protection Regulation),[8] it is evident how the pervasiveness of information technologies, mainly the *internet of things* (IoT),[9] has facilitated digital surveillance practices, making anyone using a computer device connected to the network easily traceable and monitored. In fact, the convergence and the heterogeneity of the tools connected to the network, as well as the multiplicity of subjects who revolve around the world of IoT, make the dissemination of personal information increasingly significant. In a world increasingly connected globally, there are more and more data available that can provide information capable of describing the world and people, making the interpretative algorithms more and more efficient. To this is often added the individual's lack of control of the data flow generated by the device used, frequently caused by its sudden activation,[10] and anonymity is even more difficult to maintain on the Web where identification is almost automatic. In

7 J. Rifkin, The Age of Access. The New Culture of Hypercapitalism Where All of Life is a Paid-For Experience, New York 2000. Italian translation: L'era dell'accesso, Milan 2001, p. 65.

8 The General Data Protection Regulation 679/2016 (GDPR).

9 The internet of things (IoT), an expression coined by the British researcher Kevin Ashton in 1999, expresses the transition from a network of interconnected computers to a network of connected objects of everyday life, facilitated by the development of wireless and satellite technology; S. Palanza, Internet of things, big data e privacy: la triade del futuro, Istituto Affari Internazionali, October 2016, p. 2, http://www.iai.it/sites/default/files/iai1612.pdf (accessed 19.10.20). The identification of interconnected objects occurs mostly through a unique identifier, recognizable by radio frequency (RFID); M. Iasselli, Privacy e nuove tecnologie, (in:) M. Iasselli (ed.), Diritto e nuove tecnologie. Prontuario giuridico ed informatico, Milan 2016, p. 153ff. RFID is accompanied by the use of Near Field Communication (NFC) technologies that provide two-way and short-range wireless connectivity; S. Palanza, Internet of things, *op. cit*., p. 18 ff.

10 *Ibidem*, p. 15.

this regard, an efficient use of information, mainly of big data,[11] using data mining[12] or the latest business analytics,[13] tools both paid – through the use of a particularly high number of variables that sometimes makes it difficult even to reconstruct the logic of the decision-making process[14] – to find hidden patterns and predictive rules,[15] represents an undoubted competitive advantage for companies just as it represents a new threat to privacy for individuals. It also highlights how the evaluation of the freedom and awareness of consent to processing, provided for by GDPR Art. 4, concerns only personal data, while big data tends to work on anonymous data,[16] although these data can, through appropriate correlations, become referable to very specific people.[17] In any case, the European legislative framework, while not

11 In the OECD definition, all content generated by users on the Internet is big data, including blogs, photos, videos, behavioural data, social data, geolocation data, demographic data and identification data in general: content that allows individual identification or that provides information on typical patterns of individual behaviour; M. Delmastro and A. Nicita, Big data. Come stanno cambiando il nostro mondo, Bologna 2019, p. 35. Big data can be described by means of the so-called 4Vs, that is, *volume*, *variety*, *velocity*, and *value*. For an up-to-date delineation of big data requirements, see M. Palmirani, Big data e conoscenza, "Rivista di filosofia del diritto" 2020, vol. 1, p. 77 ff. The peculiarity and potential of big data, capable of leading to a paradigm shift in the analysis of information, are found in its not having been extrapolated from representative samples by complex procedures but from the whole observed population, so that in terms of predictive efficacy, the quantity of the data prevails over the accuracy of the analysis procedure, A. Simoncini and S. Suweis, Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale, "Rivista di filosofia del diritto" 2019, vol. 1, p. 92; A.C. Amato Mangiameli, Algoritmi e big data. Dalla carta sulla robotica, "Rivista di filosofia del diritto" 2019, vol. 1, p. 112.

12 An analysis of the problems of data mining is in C. Sarra, Business Intelligence ed esigenze di tutela: criticità del c.d. Data Mining, (in:) P. Moro and C. Sarra (eds), Tecnodiritto. Temi e problemi di informatica e robotica giuridica, Milan 2017, pp. 41–63. On the use of neural networks and supervised and unsupervised learning algorithms, see A.C. Amato Mangiameli, Algoritmi, *op. cit*., p. 108.

13 Business analytics can be defined in summary as the set of tools and software applications for accessing, analyzing and viewing data that helps management quickly grasp the relevant information and control company performance in making the most effective decisions.

14 M.F. De Tullio, La privacy e i big data verso una dimensione costituzionale collettiva, "Politica del diritto" 2016, vol. 4, p. 640.

15 *Ibidem*, pp. 639, 650. A possible solution has been identified in the limitation of the maximum number of variables to be used in big data analysis, but the problem of unexpectedly extracted data, as well as additional data, would remain open, even with this hypothetical information obtained thanks to the predictive effectiveness of the algorithms used; F. Casi, Big Data ed etica dei dati, https://www.consultadibioetica.org/big-data-ed-etica-dei-dati-di-fiorello-casi/ (accessed 19.10.2020).

16 G. Della Morte, Big Data e protezione internazionale dei diritti umani. Regole e conflitti, Naples 2019, p. 161.

17 G. De Minico, Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria, "Politica del diritto" 2019, vol. 1, p. 95.

directly contemplating big data,[18] establishes some fundamental principles about the collection and use of personal information and, as recent judgments of the European Court of Justice remark, the need for effective data protection which should, in principle, prevail over economic interests,[19] considering privacy as an inviolable and essential right both of the individual and of the development of relationships.[20] The European Guarantor, too, in various opinions and initiatives, underlines the importance of a consistent regulatory application, stressing the need to seize the opportunities offered by new technologies without allowing them to determine the social values of reference.[21] The debate on privacy – which started from the protection of individual privacy towards the guarantee and control of one's own information[22] – then becomes very heated when it comes to monetization of data, that is, when it is privacy itself that becomes an economic resource and when users sell it in exchange for free services,[23] even more so considering the current indispensability of some of the data in interpersonal communications.[24] So it is possible to understand how the term 'personal data' should be interpreted in an evolutionary and extensive way,[25] passing from an individual to a collective dimension of privacy in which the subject of information self-determination becomes the concern of the whole community.[26] The challenge to be grasped – and for which the traditional rules and principles that can be deduced from international and national law often appear inadequate and obsolete – is to harmonize conflicting interests and needs, such as data protection

18 The GDPR does not make direct mention of big data, excluding from consideration data capable of profoundly affecting the expression of fundamental rights.

19 Resolution of the European Parliament of 14 March 2017, On fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement, https://www.europarl.europa.eu/doceo/document/ TA-8-2017-0076_EN.html (accessed 19.10.2020).

20 M.F. De Tullio, La privacy, *op. cit*., p. 653. We can here only mention an exemplary ruling of the German Constitutional Court of 15 December 1983, with which a real theory on informative self-determination is elaborated, built on the assumption that if the individual cannot be the exclusive owner of his/her data – which, representing social reality, are considered as neutral information – s/he has the right to control over it, representing the same manifestation of the right to the full development of his/her personality and attributing to the legislator the role of balancing assumptions and contexts that make it possible to limit the right to privacy; Bundesverfassungsgericht, 15.12.1983, 1, BvR 209/83; G. Della Morte, Big Data, *op. cit.*, p. 166.

21 European Parliament, Plenary Session of 2 March 2017, Fundamental rights implications of big data, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2017)599312 (accessed 19.10.2020).

22 G. Pascuzzi, Il diritto dell'era digitale, Bologna 2020, pp. 77–111.

23 S. Palanza, Internet of things, *op. cit*., p. 9.

24 M. Delmastro and A. Nicita, Big data, *op. cit.*, p. 24.

25 M. Orefice, I Big Data e gli effetti su privacy, trasparenza e iniziativa economica, Canterano 2018, p. 100. The ePrivacy Regulation, published in January 2017 as a proposal text, includes in the category of metadata all data other than content, but only those processed on the network and not on devices, as also noted by the Opinion of the European Privacy Guarantor 6/2017.

26 M.F. De Tullio, La privacy, *op. cit*., p. 641.

and global security,[27] obtaining an adequate balance between market logic and the essential guarantee of prevailing and non-negotiable rights.[28]

It is clear how, on these issues, the future of world competition, the stability of social structures and, finally, the maintenance of existing democratic principles are at stake. The protection of personal information in fact raises pressing ethical and legal questions which concern the protection of the fundamental rights of the person[29] and which reflect on the long-term consequences of the profiling activity and on the impacts caused by this in our lives: more and more authors, and from different research perspectives, are wondering if the risk taken by an increasingly dated profiled and automated society is not also the loss of the ability to experiment, to make mistakes, to innovate.[30] Groping for new paths means leaving the door open to error in order to change course, that is, to progress: on reflection, the ultimate risk concerning the incessant collection and processing of individual information is that of outlining a predictable and, therefore, less free society, in which the margins of individual choice, not corresponding to the interests of those who control the flow of data and recommendation algorithms, are greatly reduced.[31]

2. Polarization of Information

The participatory use in the public sphere of some types of information can have a strong social interest; just think of the sharing of information in a smart city, of the monitoring of data aimed at implementing environmental protection and, above all, of the scientific context, where pooling knowledge opens up the sharing of scientific research and its results.[32] In these cases, the collection and monitoring of information take on an extremely positive value, seeing the information rejected in favour of knowledge and equality,[33] as the basis of democratic participation that would like – as

27 On the possibility of global surveillance, see G. Ziccardi, Il libro digitale dei morti. Memoria, lutto, eternità e oblio nell'era dei social network, Milan 2017, p. 88.

28 S. Rodotà, Il mondo nella rete. Quali i diritti quali i vincoli, Rome/Bari 2019, p. 21 ff. On the balance between constitutionally protected values on the Web, see M.C. De Vivo, Comunicare in Internet. Con che diritto? "Informatica e Diritto" 2000, pp. 125–158.

29 On the link between big data and human rights, see F.A. Schreiber and L. Tanca, Etica e big data, sette principi per proteggere i diritti umani, https://www.agendadigitale.eu/cittadinanza-digitale/data-management/etica-e-big-data-sette-principi-per-proteggere-i-diritti-umani-fondamentali/ (accessed 19.10.2020).

30 A. Longo and G. Scorza, Intelligenza artificiale, *op. cit.*, pp. 136–139.

31 *Ibidem*.

32 S. Palanza, Internet of things, *op. cit.*, p. 128.

33 On the potential of big data for the prevention of human rights violations, see L. Nosari, Potenzialità e problematiche afferenti l'utilizzo dei Big Data in materia di diritti umani, https://www.cyberlaws.it/2018/big-data-e-diritti-umani/ (accessed 18.10.2020).

recalled by Art. 19 of the Universal Declaration of Human Rights – free and legally guaranteed access to knowledge and culture.[34]

In addition to the aforementioned economic and social advantages, some critical issues that pose ethical and legal challenges should be noted. A pressing factor is given by the progressive concentration of information in the hands of a few operators, a phenomenon that is reflected in the full expression of the right to inform and to be informed, consequently in the full implementation of the right to freedom and, finally, in the future of democracy. In this field, in fact, the digital platforms, called 'over the top' (OTT) or *digital giants*, having the possibility to collect and accumulate a vast amount of information released by users, give rise to a marked polarization of information power in a few private groups,[35] standing against the principle of substantial equality[36] as well as against the protection of competition and the legal construction of a transparent data-given market,[37] to the detriment of the consumer[38] and to the disadvantage of full personal and social development.

The ability of online platforms to influence the user appears effective in the political context too, as they can influence the choices of citizens, even reaching, and in some cases distorting, the *ranking* of the news in searches. The amount of information available online also corresponds to a greater amount of disinformation strategies based on *fake news*,[39] so the quality of knowledge ultimately depends on the critical and discerning ability of the end user.[40] This highlights the ethical and legal need, for the digital user, to recognize reliable information, aided by the sites themselves by providing tools to select independently.[41] Individual profiling, determined by the application of appropriate algorithms,[42] contributes to selecting crucial content for public opinion, to be reported to the individual as well as to the

34 J. Drexl, Economic Efficiency versus Democracy: On the Potential Role of Competition Policy in Regulating Digital Markets in Times of Post-Truth Politics, "Max Plank Institute for Innovation and Competition Research Paper", December 2016, no. 16, pp. 1–28.

35 M. Delmastro and A. Nicita, Big data, *op. cit*., p. 125.

36 G. De Minico, Big Data, *op. cit*., p. 113.

37 The right to the portability of personal data, structured and unstructured, enshrined in Art. 20 GDPR, seems to correspond to this logic; M. Delmastro and A. Nicita, Big data, *op. cit*., p. 31, pp. 129–130.

38 M. Orefice, I Big Data, *op. cit*., p. 11.

39 D. Talia, La società calcolabile e i big data. Algoritmi e persone nel mondo digitale, Catanzaro 2018, p. 13.

40 M. Delmastro and A. Nicita, Big data, *op. cit*., p. 93. The Control Authority for Communications Guarantees has launched a monitoring table on the self-regulation put in place by search engines and social networks, anticipating the work started by the European Commission with the establishment of the High-Level Group on Fake News and Online Disinformation.

41 L. Palazzani, Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto, Rome 2020, p. 21.

42 A.C. Amato Mangiameli, Algoritmi, *op. cit*., p. 109.

political agenda.[43] In the creation of a *filter bubble*,[44] aimed at showing the user the information that the algorithm has calculated for him as potentially interesting,[45] all the asymmetry between the provider of the information service and the user is shown. Obviously, in fact, the abstract communicative symmetry on the Web does not imply an effective parity in sharing knowledge, but rather confirms the social disparity between those who hold information power and those who do not. Thus 'despite the enormous capacity that the digital medium has in distributing data and information to everyone, indiscriminately and at the same instant, everyone ends up amplifying themselves and does not contribute to the collective amplification of criticism and protest'.[46]

This condition is aggravated by the frequent lack of transparency of the criteria set underlying the functioning of the algorithm.[47] Therefore, the importance of the *explainability* of the results produced by artificial intelligence algorithms should be put in evidence, in addition to the *knowability* of the automated decision-making process and of the data used in it,[48] avoiding any possible lack of responsibility attributed to the interpretative capacity of the algorithms used[49] since 'it is the principle of equality that claims responsibility'.[50] The principle of *transparency*, which in this case concerns the possibility of knowing the logic behind every decision taken with the help of artificial intelligence, tracing the calculations to a humanly understandable form,[51] is particularly relevant in fully automatically decided proceedings, producing legal effects and significantly affecting personal rights and freedoms,[52] and raising pressing ethical questions about the possible dangers of algorithmic discrimination against individuals or social groups that are external to the algorithmic logic and so marginalized through self-fulfilling predictions.[53] In fact, the risk that artificial intelligence could

43 M. Delmastro and A. Nicita, Big data, *op. cit*., p. 91.

44 E. Pariser, The Filter Bubble. What the Internet Is Hiding From You, New York 2011; Z. Bauman and T. Lyon, Liquid Surveillance. A Conversation, Cambridge 2013. Italian translation: Sesto potere. La sorveglianza nella modernità liquida, Rome/Bari 2015, pp. 118–119.

45 A.C. Amato Mangiameli, Algoritmi, *op. cit*., p. 109.

46 D. Talia, La società calcolabile, *op. cit*., p. 11.

47 *Ibidem*, p. 97.

48 M. Palmirani, Big data e conoscenza, *op. cit*., pp. 73–92.

49 S. Rodotà, Il mondo, *op. cit*., p. 39. In this regard, the USACM Statement on Algorithmic Transparency and Accountability, 12 January 2017, https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_ algorithms.pdf (accessed 19.10.2020), is very significant, as is the Resolution of the European Parliament of 16 February 2017, *op. cit*.

50 G. Teubner, Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten, 'Archiv für civilistiche Praxis' 2018, pp. 155–205. Italian translation: Soggetti giuridici digitali? Sullo *status* privatistico degli agenti *software* autonomi, Naples 2019, p. 84.

51 A.C. Amato Mangiameli, Algoritmi, *op. cit*., p. 120.

52 M. Palmirani, Big data e conoscenza, *op. cit*., pp. 73–92.

53 M.F. De Tullio, La privacy, *op. cit*., p. 662.

discriminate against minorities and weak subjects – through the so-called *bias*, that is, algorithmic prejudices that can be introduced right from the planning stage of the collection and automated processing of information – constitutes one of the main ethical problems analyzed by the scientific community.[54] This could represent a counterintuitive concept, given that machines and algorithms have no prejudices or conflicts of interest nor make mistakes, yet this reasoning has in many cases shown a flaw, since the algorithms were always designed by men and trained on personal data, and it is therefore possible that they have incorporated prejudices and social discrimination with the possible aggravation of not subsequently being subjected to human scrutiny and correction.[55] Special attention has been paid to these problems by the Treaty on European Union, expressing the criteria of non-discrimination, autonomy and justice (Art. 2), and by the Charter of Fundamental Rights of the Union which underlines the relevance of principles such as human dignity, justice, non-discrimination and informed consent. On these issues, the European Commission for the Effectiveness of Justice of the Council of Europe adopted, in December 2018, a *European Ethical Charter for the use of artificial intelligence in justice systems and related environments* aimed at promoting a prescriptive approach targeted at securing information and the free choice of social actors.[56] The central question, ethical and at the same time legal, becomes how to balance the prescriptive function of law with the logic underlying policies based on the detailed collection of information, endorsing economic interests or state social control.[57] From this perspective, the protection of constitutionally guaranteed values,[58] such as respect for the dignity of the human person and the guarantee of moral and juridical equality, appears to prevail over the identification of any market models.[59] This would mark an important step towards a properly interactive world, inaugurating an effective model of digital citizenship and generating a new form of civil solidarity fuelled by information.[60]

54 A. Longo and G. Scorza, Intelligenza artificiale, *op. cit*., p. 123.

55 *Ibidem*, p. 119.

56 G. Pascuzzi, Il diritto, *op. cit.*, p. 296–299.

57 G. Della Morte, Big Data, *op. cit*., p. 9. The subjects able to carry out an effective concentration of information are represented not only by OTT but also by authoritarian governments and government security agencies on an anti-terrorist mission: on the numerous legislative initiatives, which multiplied mainly after 11 September 2001 and aimed at countering international terrorism, see S. Palanza, Internet of things, *op. cit*., p. 14.

58 A. Simoncini and S. Suweis, Il cambio di paradigma, *op. cit*., p. 103.

59 P. Perlingeri, Il diritto civile nella legalità costituzionale, Naples 1991, pp. 444–445.

60 M. Orefice, I Big Data, *op. cit*., p. 25.

3. Algorithms and Artificial Intelligence: Some Ethical and Legal Considerations

The growing use of personal information, as well as of the knowledge that can be extracted from big data, brings out a further ethical and legal problem determined by the fact that the procedures for extracting significant information from data are united by the use of increasingly sophisticated machines and complex algorithms, capable of 'learning' from information but often 'opaque', generating a *black box* effect that makes it difficult to understand the reasons for the decisions taken automatically.[61] In other words, the lack of transparency in the algorithm's operating criteria does not allow us to understand the mechanisms behind profiling, prediction and standardization calculations.[62] Consequently, analysts often make their own decisions not because they have fully understood the logic of the connection in the data they have found, but because they know well how the most recurrent correlations have a good chance of recurring even in future cases.[63] Sometimes, these decisions are not interpretable, that is, they cannot logically be understood, as the algorithms used employ a particularly large number of variables, too many for the calculation to be reconstructed a posteriori by a human mind: in these hypotheses, the very nature of the procedure expresses the impossibility of giving an account of the decisions, and this contrasts, as seen, with the interest of any subjects who suffer negative effects and who would have reasonable claims to oppose them.[64] So the algorithmic logic of the predictive model – which informs the process of extraction, collection and storage of big data – in addition to profoundly modifying the traditional mechanisms of power by introducing new decision-makers and new powers,[65] raises unprecedented ethical and juridical questions about the possible dangers of algorithmic discrimination against groups socially marginalized through self-fulfilling predictions,[66] demonstrating that predictive analysis can lead to detrimental effects regardless of the error or inaccuracy of the algorithmic forecast.[67] This problem is particularly relevant if one only thinks of the fact that today technology is no longer just a tool to achieve goals decided by a human subject, but itself makes decisions that are in some cases relevant to freedom and to individuals, so that it becomes essential to guarantee an explanation of *why* the machine has made that specific decision.[68] All the relevance of the principle of transparency is highlighted, which is realized

61 G. Pascuzzi, Il diritto, *op. cit.*, p. 273.
62 L. Palazzani, Tecnologie dell'informazione, *op. cit.*, p. 33.
63 M.F. De Tullio, La privacy, *op. cit.*, p. 639.
64 *Ibidem*, p. 640.
65 S. Rodotà, Il diritto di avere diritti, Rome/Bari 2015, pp. 394–395.
66 M.F. De Tullio, La privacy, *op. cit.*, p. 662.
67 G. De Minico, Big Data, *op. cit.*, pp. 93–97.
68 A. Simoncini and S. Suweis, Il cambio di paradigma, *op. cit.*, pp. 92–93.

in the possibility of knowing the logic behind each decision taken with artificial intelligence systems, bringing it back to a form understandable for humans.[69] In this sense, the functional transparency of the algorithm would seem partly satisfied in the presence of its selective disclosure, that is, suitable to cover only the main lines of the algorithm to allow interested parties to understand the ultimate goals of the predictive mechanism, without unjustifiably cancelling the intellectual property right of the legitimate owner of the algorithm.[70] This also seems to suggest an innovative criterion of liability, replacing or in addition to the criterion of civil liability for negligence, and having a justifying title in a business risk in the event of a harmful forecast as discriminatory towards certain categories of subjects, given that predictive analysis can have detrimental effects even regardless of the error or inaccuracy of the forecast. In other words, the inevitable factor of uncertainty which, paradoxically, characterizes algorithmic prediction should lead to an increase in responsibility for its user, having to respond regardless of fault or wilful misconduct, and underlining how the massive nature of information collection involves the damage in a new way of being, no longer limited to the single individual but widespread in the community.[71] Finally, it becomes essential that law and ethics move from the fundamental distinction between what can be programmed and what instead escapes any planning activity as it pertains to the most specific sphere of human choice and reflection.[72]

4. Technological Enhancement and Human Enhancement: Some Open Questions

There are many fields of the application of artificial intelligence to law – the analysis and preparation of deeds and documents, as well as predictive analysis, are just two examples – and some of these raise pressing ethical as well as legal questions, as in the case of automated legal decision-making. By broadening our gaze, we can discover the many sectors in which artificial intelligence unfolds:[73] we have sophisticated machines which, thanks to complex algorithms, are able to learn and decide independently,[74] although artificial intelligence is generally still 'restricted', that is, capable of achieving only very specific purposes.[75] On the other hand, technological cognitive enhancement, supported by the phenomenon of technological

69 A.C. Amato Mangiameli, Algoritmi, *op. cit*., p. 120.
70 G. De Minico, Big Data, *op. cit*., pp. 93–98.
71 *Ibidem*.
72 A. C. Amato Mangiameli, Algoritmi, *op. cit*., p. 123.
73 G. Pascuzzi, Il diritto, *op. cit.*, p. 303.
74 *Ibidem*, p. 307.
75 M. Tegmark, Life 3.0. Being Human in the Age of Artificial Intelligence, London 2017. Italian translation: Vita 3.0. Esseri umani nell'era dell'intelligenza artificiale, Milan 2018, p. 113.

convergence,[76] is developing not only on the information level, but also in the more properly human field, taking on a relevant regulatory significance.[77] Obviously, these research perspectives are necessarily interdisciplinary and still uncertain due to the partiality of information and, in some cases, the lack of experimentation on humans, but they proceed rapidly, united by a deep consideration of the possible technological transformations of humans.[78] So philosophical, ethical and juridical reflection, without prejudice to the guarantee of the pluralism of values that constitutes democratic and modern societies, is called into question in developing an effective conceptual framework and interpretation of these problems, with particular attention given to the limits to be placed on human manipulation and alteration, in the double sense of the artificialization of the human and the humanization of technology.[79]

We speak of *roboethics* to indicate the study of the interactions between intelligent machines and between them and human beings, and we show an *ethical approach by design* to counter the lack of an ethical dimension in IT tools and the freeing of their actions from any ethical evaluation, placing the necessary respect for human dignity at the centre of reflection, both moral and juridical, instead.[80]

In this field, some value charts have been developed with the aim of incorporating core values into algorithms, created in such a way that robots conform to them;[81] first of all human dignity, transparency (understood as the control and predictability of autonomous systems), responsibility (prudence in the face of potential dangers), justice and solidarity (to guarantee equal access to resources and democratic participation). This is also the direction of the Recommendation CM/Rec (2020) 1 of the Committee of Ministers to Member States on the human rights impacts of algorithmic systems, which advocates the diffusion of guidelines and ethical standards concerning the design, development and implementation of algorithmic systems that guarantee respect for the rights recognized by the European Convention on Human Rights.[82] The risk of the autonomy of self-learning algorithms is particularly incisive, and it opens up from individual law to collective law, from

76 G. Pascuzzi, Il diritto, *op. cit.*, pp. 59–66.

77 L. Palazzani, Il potenziamento umano. Tecnoscienza, etica e diritto, Torino 2015, pp. 122–139.

78 *Ibidem*, p. 126.

79 *Ibidem*, p. 127.

80 P. Perri, Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica, Milan 2020, p. 133.

81 European Parliament, Robotics Charter of 16 February 2017, and the European Group on Ethics in Science and New Technologies at the European Commission, March 2018, Statement on Artificial Intelligence, Robotics and Autonomous Systems, http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf (accessed 19.10.2020).

82 Recommendation CM/Rec (2020) 1 of the Committee of Ministers to Member States on the human rights impacts of algorithmic systems, https://search.coe.int/cm/pages/result_details.aspx?objectid= 09000016809e1154 (accessed 09.11.2020).

civil liability to social security:[83] pressing unknowns weigh on the so-called 'ethical choices' of artificial agents and on the configuration of innovative hypotheses of responsibility to attribute to the acts they commit.[84] Just think of the 'ethical choices' of automatic pilots, which essentially translate the definitions of the algorithms through which the manufacturers of automatic vehicles set the means of transport, for the management of the most unpredictable and complex driving situations. In these cases, a proactive rather than a reactive approach is to be preferred, investing in safety research aimed at preventing the occurrence of even a single accident.[85] It is essential that the more we rely on technology the more it must be 'robust', that is, trustworthy in its manifestations.[86] In fact, if society attributes new decision-making spaces to autonomous decision-makers, it is obliged to introduce *new* forms of responsibility, detached from mere considerations of efficiency, the reduction of transaction costs and utilitarian evaluations, but specifically tailored to the decision-making risk of such autonomous agents.[87] These short reflections show all the complexity of the relationship between technology, ethics and law, such that the dimension of values is found not only in the definition of the purposes that technology should help to pursue but also in the production of the technology itself.[88]

Conclusions

The pervasiveness of information technologies as well as the use of sophisticated techniques for the extraction of knowledge from data – fundamental tools in the information society – have facilitated digital surveillance practices, making anyone using a computer device connected to the network easily traceable and monitored, which raises pressing ethical and legal questions in respect to the right to privacy, today rightly considered as a fundamental right of the person.

Further unknowns, which mainly come from the increased ability to extract and interpret big data, derive from the progressive concentration of knowledge in the hands of a few 'digital giants', giving rise to pressing ethical and legal problems in order to respect the principles of equality and sharing of knowledge at the foundation of an effective democratic society. The central question, then, becomes how to balance the prescriptive function of law with policies based on the diffused collection

83 G. Teubner, Soggetti giuridici, *op. cit.*, p. 14.

84 G. De Anna, Automi, responsabilità e diritto, 'Rivista di filosofia del diritto' 2019, vol. 1, pp. 125–142.

85 M. Tegmark, Vita 3.0, *op. cit.*, p. 129.

86 *Ibidem.*

87 G. Teubner, Soggetti giuridici, *op. cit.*, pp. 84–94.

88 B. Bisol, A. Carnevale and F. Lucivero, Diritti umani, valori e nuove tecnologie. Il caso dell'etica della robotica in Europa, "Metodo. International Studies in Phenomenology and Philosophy" 2014, vol. 1, p. 248.

of information and, from this perspective, the protection of constitutionally guaranteed values – primarily respect for the dignity of the human person; moral and legal equality; freedom of opinion, press, assembly, association and religion. Here the right to participate in the choices that affect everyone appears to prevail over the identification of any market models.

Finally, the link between ethics, law and information technologies becomes particularly delicate when the latter are addressed to so-called 'human enhancement', taking on a relevant regulatory significance that requires a necessarily interdisciplinary perspective of analysis and discussion which is capable of guaranteeing, promoting and enhancing justice, social solidarity and the pluralism of values that constitutes modern democratic societies. It is evident, in fact, that developments in artificial intelligence and digital technology are not just technical issues but closely affect people, their lives and social relationships: for these reasons, they oblige us to ask ourselves about the ever-changing balances between automation and human decision, control and privacy, efficiency and security that a society is ready to accept. These are fundamental themes of common living, the regulation of which cannot be left either to the market or to technocracy alone, as it requires the essential intermediation of democratic institutions which can consider how, in a pluralist society, the different positions of social actors should be protected as much as possible, even when they can be strongly discordant or even incompatible with each other.[89] It therefore seems necessary to start an ethical and juridical reflection, inserted into the framework of democratic debate, which is capable of enhancing every different perspective without imposing any of them, and to dynamically define the field of acceptability of emerging technologies.[90]

REFERENCES

Amato Mangiameli A. C., Algoritmi e big data. Dalla carta sulla robotica, "Rivista di filosofia del diritto" 2019, vol. 1.

Bauman Z. and Lyon T., Liquid Surveillance. A Conversation, Cambridge 2013. Italian translation: Sesto potere. La sorveglianza nella modernità liquida, Rome/Bari 2015.

Bisol, B., Carnevale, A. and Lucivero F., Diritti umani, valori e nuove tecnologie. Il caso dell'etica della robotica in Europa, "Metodo. International Studies in Phenomenology and Philosophy" 2014, vol. 1.

Casi F., Big Data ed etica dei dati, https://www.consultadibioetica.org/big-data-ed-etica-dei-dati-di-fiorello-casi/.

De Anna G., Automi, responsabilità e diritto, "Rivista di filosofia del diritto" 2019, vol. 1.

Della Morte G., Big Data e protezione internazionale dei diritti umani. Regole e conflitti, Naples 2019.

89 *Ibidem*, p. 236.
90 *Ibidem*, p. 237.

Delmastro M. and Nicita A., Big data. Come stanno cambiando il nostro mondo, Bologna 2019.

De Minico G., Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria, "Politica del diritto" 2019, vol. 1.

De Tullio M. F., La privacy e i big data verso una dimensione costituzionale collettiva, 'Politica del diritto' 2016, vol. 4.

De Vivo M. C., Comunicare in Internet. Con che diritto? "Informatica e Diritto" 2000.

Drexl J., Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of post truth politics, "Max Plank Institute for Innovation and Competition Research Paper", December 2016, no. 16.

Iasselli M., Privacy e nuove tecnologie, (in:) M. Iasselli (ed.), Diritto e nuove tecnologie. Prontuario giuridico ed informatico, Milan 2016.

Longo A. and Scorza G., Intelligenza artificiale. L'impatto sulle nostre vite, diritti e libertà, Milan 2020.

Nosari L., Potenzialità e problematiche afferenti l'utilizzo dei Big Data in materia di diritti umani, https://www.cyberlaws.it/2018/big-data-e-diritti-umani/.

Orefice M., I Big Data e gli effetti su privacy, trasparenza e iniziativa economica, Canterano 2018.

Palanza S., Internet of things, big data e privacy: la triade del futuro, Istituto Affari Internazionali October 2016, http://www.iai.it/sites/default/files/iai1612.pdf.

Palazzani L., Il potenziamento umano. Tecnoscienza, etica e diritto, Torino 2015.

Palazzani L., Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto, Rome 2020.

Palmirani M., Big data e conoscenza, "Rivista di filosofia del diritto" 2020, vol. 1.

Pariser E., The Filter Bubble. What The Internet Is Hiding From You, New York 2011.

Pascuzzi G., Il diritto dell'era digitale, Bologna 2020.

Perlingeri P., Il diritto civile nella legalità costituzionale, Naples 1991.

Perri P., Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica, Milan 2020.

Rifkin J., The Age of Access: The new Culture of Hypercapitalism, Where All of Life is a Paid-for-Experience, New York 2000. Italian translation: L'era dell'accesso, Milan 2001.

Rodotà S., Il diritto di avere diritti, Rome/Bari 2015.

Rodotà S., Il mondo nella rete. Quali i diritti quali i vincoli, Rome/Bari 2019.

Sarra C., Business Intelligence ed esigenze di tutela: criticità del c.d. Data Mining, (in:) P. Moro, C. Sarra (eds.), Tecnodiritto. Temi e problemi di informatica e robotica giuridica, Milan 2017.

Schreiber F.A., Tanca L., Etica e big data, sette principi per proteggere i diritti umani, https://www.agendadigitale.eu/cittadinanza-digitale/data-management/etica-e-big-data-sette-principi-per-proteggere-i-diritti-umani-fondamentali/.

Simoncini A. and Suweis S., Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale, "Rivista di filosofia del diritto" 2019, vol. 1.

Talia D., La società calcolabile e i big data. Algoritmi e persone nel mondo digitale, Catanzaro 2018.

Tegmark M., Life 3.0. Being Human in the Age of Artificial Intelligence, London 2017; Italian translation: Vita 3.0. Esseri umani nell'era dell'intelligenza artificiale, Milan 2018.

Teubner G., Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten, "Archiv für civilistiche Praxis" 2018, Italian translation: Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi, Naples 2019.

Wnukiewicz-Kozłowska A., The Right to Privacy and Medical Confidentiality – Some Remarks in Light of ECtHR Case Law, "Białostockie Studia Prawnicze" 2020, vol. 25, no. 2.

Zanichelli M., Affidabilità, diritti fondamentali, centralità dell'essere umano: una strategia europea per l'intelligenza artificiale, "i-lex" 2019, vol. 12, http://www.i-lex.it/articles/volume12/fascicolo1-3/zanichelli.pdf.

Ziccardi G., Il libro digitale dei morti. Memoria, lutto, eternità e oblio nell'era dei social network, Milan 2017.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.02

Received: 19.12.2020
Accepted: 25.03.2021

Rafał Rejmaniak
University of Białystok, Poland
r.rejmaniak@uwb.edu.pl
ORCID ID: https://orcid.org/0000–0003-1908–5844

Bias in Artificial Intelligence Systems

Abstract: Artificial intelligence systems are currently deployed in many areas of human activity. Such systems are increasingly assigned tasks that involve taking decisions about people or predicting future behaviours. These decisions are commonly regarded as fairer and more objective than those taken by humans, as AI systems are thought to be resistant to such influences as emotions or subjective beliefs. In reality, using such a system does not guarantee either objectivity or fairness. This article describes the phenomenon of bias in AI systems and the role of humans in creating it. The analysis shows that AI systems, even if operating correctly from a technical standpoint, are not guaranteed to take decisions that are more objective than those of a human, but those systems can still be used to reduce social inequalities.
Keywords: AI discrimination, AI fairness, algorithmic bias, artificial intelligence

Introduction

Technological solutions based on artificial intelligence (AI) are being used more and more widely in various spheres of human activity. AI systems are deployed in both the private and the public sectors. The widespread use of such solutions is motivated by the potential benefits, which are hard to overestimate – from making production processes more efficient or analysing large quantities of data at speeds far exceeding human capabilities to forecasting future events. One of the frequently cited properties of AI systems, said to give them an advantage over humans in performing certain types of tasks, is the greater objectivity of their 'decisions' and

their insusceptibility to the influence of subjective feelings and emotions.[1] There is no doubt that from a technical point of view, in the case of tasks requiring precision, repeatability and the processing of large quantities of data in a short time, AI systems will generally outperform humans. This does not mean, however, that such systems are guaranteed to carry out the tasks entrusted to them in a way that can be regarded as appropriate from a social perspective.

From the growing number of studies concerning this problem, it is becoming clear that even AI systems can be subject to bias, and in the longer term this may lead to discrimination against individuals or even entire social groups.[2] The problem is acknowledged by various bodies seeking to establish legal and ethical frameworks for the development of artificial intelligence, both nationally and internationally.[3] The aim of this article is to describe the phenomenon of bias in AI systems and to show that AI systems, even when biased, can be useful for reducing social inequalities. For the purposes of this work, the term 'bias' is taken to mean simply a deviation from the norm,[4] understood as a commonly accepted and agreed standard, making it a broader concept than 'discrimination'. It is worth noting that these very standards may show a discriminating nature on their own, having roots in beliefs and prejudices found in society or being politically motivated.

1. The Notion of Artificial Intelligence

'Artificial intelligence' is a notion that does not yet have a single generally accepted definition. For the purposes of this work, artificial intelligence will be understood as proposed by the High-Level Expert Group on Artificial Intelligence – as 'software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing

1 P. Hacker, Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law, "Common Market Law Review" 2018, vol. 55, pp. 1143–1144.

2 See R. Rodrigues, Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities, "Journal of Responsible Technology" 2020, vol. 4, p. 3.

3 See J. Fjeld, N. Achten, H. Hilligoss, A. Nagy and M. Srikumar, Principled Artificial Intelligence. Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI, Cambridge 2020, pp. 47–52.

4 D. Danks and A.J. London, Algorithmic Bias in Autonomous Systems, "Proceedings of the 26th International Joint Conference on Artificial Intelligence (IJCAI 2017)", p. 2, https://www.cmu.edu/dietrich/philosophy/docs/ london/IJCAI17-AlgorithmicBias-Distrib.pdf (accessed 06.02.2021).

how the environment is affected by their previous actions'.[5] The authors of this definition specify the meaning of a 'decision' as 'any act of selecting the action to take', and this 'does not necessarily mean that AI systems are completely autonomous. A decision can also be the selection of a recommendation to be provided to a human being, who will be the final decision maker.'[6]

In contrast to ordinary algorithms, which involve the sequential completion of predefined steps, a fundamental feature of AI is the ability to 'learn'. In this process, known as machine learning, external empirical data are used to create and update rules for the improved handling of similar data in the future, and to express these rules in a comprehensible, symbolic form.[7] It is not the aim of this article to present the techniques of machine learning,[8] but it is necessary to make two remarks to enable understanding of the problems of AI bias that are to be discussed below.

First, machine learning may take the form of supervised, unsupervised or reinforcement learning.[9] In the first case, the data used to train the AI system are labelled. The system analyses the input data and determines relationships between them. If it makes an incorrect classification, it is informed of that fact and will modify its hypotheses.[10] Unsupervised learning uses a pool of unlabelled training data; the task of the AI system is to find, independently, non-trivial relationships in the data. In such cases, as a rule, the trainers do not have knowledge of the final outcome of the learning process. In reinforcement learning, on the other hand, for every correct classification the system receives a 'reward' (for example, its goal is to earn as many points as possible, and for each correct identification of data it is awarded points, while for an incorrect identification it has points taken away). Some AI systems are brought into use after their training is complete, whereas others continue to learn for the whole time that they are in use. An example of the latter type is Google Translate.[11]

Second, while various techniques are used for training AI systems, one of the most popular currently is deep learning, based on multiple layers of artificial neural networks. An artificial neural network is a simplified mathematical model

5 High-Level Expert Group on Artificial Intelligence (appointed by the European Commission in June 2018), A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines, Brussels 2019, p. 6.

6 *Ibidem*, p. 3.

7 D. Michie, Methodologies from Machine Learning in Data Analysis and Software, "The Computer Journal" 1991, vol. 34, no. 6, p. 562.

8 See e.g. M. Flasiński, Wstęp do sztucznej inteligencji, Warsaw 2020; L. Rutkowski, Metody i techniki sztucznej inteligencji, Warsaw 2012.

9 M.A. Boden, Sztuczna inteligencja. Jej natura i przyszłość, trans. T. Sieczkowski, *Łódź* 2020, pp. 59–60.

10 *Ibidem*, p. 60.

11 G. Massey and M. Ehrensberger-Dow, Machine Learning: Implications for Translator Education, "Lebende Sprachen" 2017, vol. 62, no. 2, p. 301.

of the structure of the brain.[12] The artificial neurons that form such a network receive input signals, each signal being multiplied by a corresponding numerical value called a weight. If an activation threshold is exceeded, the neuron transmits a signal which becomes an input signal for neurons in the next layer.[13] In this case, learning consists of determining appropriate weights for the various input signals. A significant issue concerning deep learning is the presence of hidden layers between the input and output layers – the networks themselves lack the ability to explain the decision-making process.[14] While it is still possible to determine what weights have been assigned to particular input signals and to repeat the training in case of an unsatisfactory result,[15] it is no longer possible to establish *why* the system assigned weights as it did.

2. Types of Bias in AI Systems

The phenomenon of AI bias is a complex one, and may be caused by a variety of factors arising at different stages of the training and operation of such a system. The first group of factors relates to the data used as a basis for training or for the making of decisions or predictions. A second group is related to the construction of the system itself. The third group consists of factors affecting the user who interprets the system's decisions or predictions.

An AI system is trained by supplying it with data, which may or may not be labelled. The quality of the training data will determine how the system subsequently functions. Even at this stage, human decisions can introduce bias into the system. It is humans who select the data to be included in the training set, and so if these data are chosen in a biased manner, then the system's subsequent decisions will be similarly biased.[16] For example, if the training set for a face recognition system consists mostly of photographs of white men, then a system trained on that set will be capable of recognizing white male faces much more effectively than those of black women.[17] Lower accuracy in facial recognition does not necessarily mean that it bears a nature of bias. Only if such a system is utilized in a particular context may its use be related to partiality, especially when its operation could influence the situation of the individual who is the subject of a decision.

12 M. Flasiński, Wstęp, *op. cit.*, p. 161.

13 A. Kasperska, Problemy zastosowania sztucznych sieci neuronalnych w praktyce prawniczej, „Przegląd Prawa Publicznego" 2017, no. 11, p. 25.

14 *Ibidem*, p. 27.

15 M. Flasiński, Wstęp, *op. cit.*, p. 163.

16 M. Coeckelbergh, AI Ethics, Cambridge/London 2020, pp. 130–131; W. Barfield and U. Pagallo, Advanced Introduction to Law and Artificial Intelligence, Cheltenham/Northampton 2020, p. 25.

17 M.S. Cataleta and A. Cataleta, Artificial Intelligence and Human Rights: An Unequal Struggle, "CIFILE Journal of International Law" 2020, vol. 1, no. 2, p. 46.

The problem of data bias can take yet another form, being rooted more deeply in the inequalities existing in society as a whole. An example here is COMPAS, a criminological risk assessment system based on AI algorithms that was tested in the United States. The system achieved 70% accuracy,[18] although its code remained a trade secret.[19] An investigation by journalists from the ProPublica website, covering persons charged with offences in Florida in 2013–14, showed – using reverse engineering – that COMPAS made false positive predictions twice as often in relation to black people and false negatives twice as often in relation to whites,[20] even though its creators claimed that the system did not consider race as a relevant feature.[21] It was further shown that HART, a similar prediction system used in the United Kingdom, also took decisions of a tendentious and discriminatory nature.[22] According to Hannah Fry, this type of bias is inevitable from a statistical point of view, since in the case of certain types of offence, black citizens in the United States are arrested much more often than whites, even though the percentages of offences committed are in fact similar in both populations.[23] Here the bias in the AI system results from the prejudices existing in society itself, which are reflected in the statistical data used to train the system. Although the act of comparing the criminality of black and white people may be controversial, having in mind its controversial political background, it is established that the sheer mechanism for AI functioning does not raise any doubts. For example, if 80% of a group's individuals can be characterized by a certain feature, it is most probable that the AI system is going to attribute a high value to it, no matter what type of a feature it is.

Controversies of a more general nature can also be attributed to the use of systems such as COMPAS. Criminological prognosis, not to mention the adjudication of

18 T. Brennan, W. Dieterich and B. Ehret, Evaluating the Predictive Validity of the COMPAS Risk and Needs Assessment System, "Criminal Justice and Behavior" 2009, vol. 36, no. 1, p. 31.

19 H. Fry, Hello World. Jak być człowiekiem w epoce maszyn, trans. S. Musielak, Krakow 2019, p. 87.

20 J. Angwin, J. Larson, S. Mattu and L. Kirchner, Machine Bias, ProPublica 2016, https://www.propublica.org/ article/machine-bias-risk-assessments-in-criminal-sentencing (accessed 19.03.2021). ProPublica journalists conducted an analysis of 10,000 accused individuals from Broward County, Florida. It has been checked whether those individuals behaved as predicted by the COMPAS system's prognosis for two consecutive years. What is more, the analysis showed that in the case of a similarity between variables such as previously committed crimes, age and sex, accused black defendants have been 45% more likely to get misclassified as higher risk than white defendants. Detailed methodology has been presented by the authors: J. Larson, S. Mattu, L. Kirchner and J. Angwin, How We Analyzed the COMPAS Recidivism Algorithm, ProPublica 2016, https://www.propublica. org/article/how-we-analyzed-the-compas-recidivism-algorithm (accessed 19.03.2021).

21 A. Yapo and J. Weiss, Ethical Implications of Bias in Machine Learning, "Proceedings of the Annual Hawaii International Conference on System Sciences" 2018, p. 5368.

22 M. Dymitruk, Sztuczna inteligencja w wymiarze sprawiedliwości?, (in:) L. Lai and M. Świerczyński (eds.), Prawo sztucznej inteligencji, Warsaw 2020, p. 283.

23 H. Fry, Hello World, *op. cit.*, pp. 92–94.

guilt and penalty, should take into consideration the circumstances of a specific case. Taking into account only the statistical models would distort the fundamental rule of criminal law – the individualization of criminal liability. Because of the above, such tools could only serve an auxiliary role for the adjudication process.

This type of bias in AI systems may lead in the end to a damaging feedback loop that petrifies or exacerbates existing inequalities. Such a system makes decisions based on previously gathered data. Those decisions are implemented, generating further strings of data that enhance the system. Thus the functioning of the system itself is generating data which is used to update its predictive model. This phenomenon is explained by C. O'Neil with an example of the PredPol system. She points out that in the case of predictive systems, a situation may be reached where the system identifies certain geographical areas as being more likely than others to experience crime. Police officers are sent to those areas, and because they happen to be there, will tend to arrest persons committing relatively minor offences. The same types of offences are not recorded in other areas, where (because of the system's predictions) officers were not sent, and therefore are not included in the police statistics. The same statistical data are fed into the AI system, which uses them to update its predictive model,[24] treating places where crimes have been recorded as potential crime areas and those where crimes have not been recorded as being less in need of the police's attention. When the system operates in this way, it produces self-fulfilling prophecies.

A predictive system on its own does not create crime. What it does is point out areas where officers' attention should be focused. It is especially important from the perspective of the optimal use of human resources, which are always limited. The problem with predictive systems does not lie in the fact that officers discover minor offences (all deviations from the criminal law norm should meet adequate state reaction) but with having certain geographical areas deemed by the system to be especially at risk of crime. It may lead to a situation where such areas could be overrated by the system due to the system's data generation, with other regions with a higher crime rate somehow neglected.

Moreover, the use of such systems may also have negative social consequences. Disproportionate police surveillance carried out in poor districts may lead to inhabitants' loss of trust towards the officers and also towards each other, and it is worth noting that trust is crucial in such places.[25] Such operation of the system may result in social exclusion based on domicile and stereotypes connected with inhabitants of particular districts dubbed as high-crime areas. Such prejudices could impact the life of an individual in many ways, e.g. during a job search or the possibility of receiving a loan.

24 C. O'Neil, Broń matematycznej zagłady. Jak algorytmy zwiększają nierówności i zagrażają demokracji, trans. M.Z. Zieliński, Warsaw 2017, pp. 128–129.

25 M. Coeckelbergh, AI Ethics, *op. cit.*, p. 128.

The above does not mean that the use of predictive systems to fight crime should be entirely discontinued. Crime forecasting is not a new phenomenon, and criminology experts have made attempts, with varying degree of success, to predict the future shape of crime rates and types. The use of a predictive system could help identify areas particularly vulnerable to crime. It may be especially important for crime categories which are related to area and infrastructure, such as burglary, the consumption of alcohol in public places, property damage, etc. Directing officers to these places may allow the creation of hot spots and in the future the implementation of relevant infrastructural solutions (e.g. city lighting or CCTV monitoring). In a case like this, it would make a predictive system one of the integrated components of a larger crime prevention system.

Another solution would be to limit the use of the AI system to only forecasting minor offences, leaving out more serious ones, which usually occur less often. It may seem, though, that no matter how the system is implemented, it would be necessary to periodically verify its accuracy and further update predictive model data with information gathered from other areas, e.g. obtained via periodic analogous intensification of patrolling in random sectors of the city.

Even if a society has overcome the problem of discrimination against a particular group, this does not mean that an AI system will be free of data bias. Such systems are trained using large quantities of data (big data), some of which are historical. Thus, if there is bias in the historical data, a system trained on those data may still end up biased. This phenomenon is known as *historic bias*.[26] Theoretically it is possible to train a system on current data, omitting the defective historical data, but in practice this approach may leave too small a training set.[27] Decisions of the AI system may still be biased. This could be attributed to the limited validity of the model, a result of it being based on a small data pool.

In the case of systems whose learning ends before they are brought into use, the data used for training are to some extent subject to control by the people responsible for the training process. However, other systems continue to learn while they are in use. This enables the system to acquire new data and to modify its behaviour continuously so as to perform its tasks in an optimum manner. The data obtained by such systems may also prove defective. There are known cases where users deliberately fed discriminatory data into the system. One of the best-known examples is the Tay bot, launched by Microsoft in 2016, which was supposed to simulate a lively, happy teenage girl on Twitter. The bot was designed to create its own tweets, learning from interactions with other users. After a few hours of being deliberately fed controversial

26 F. Lattimore, S. O'Callaghan, Z. Paleologos, A. Reid, E. Santow, H. Sargeant and A. Thomsen, Using Artificial Intelligence to Make Decisions: Addressing the Problem of Algorithmic Bias. Technical Paper, Australian Human Rights Commission, Sydney 2020, pp. 33–34.

27 *Ibidem*, p. 39.

content, the bot began to publish tweets of a racist, sexist and antisemitic nature, and Microsoft therefore decided to shut it down.[28]

Sometimes the bias in an AI system may be a consequence of the way the system itself is constructed. According to David Danks and Alex John London, this situation may be reached when data are processed using a statistically biased estimator.[29] In some cases the use of such estimators may be justified: for instance, to increase the accuracy and reliability of the results when a system is trained on a small amount of data.[30]

There are also solutions that deliberately produce a given type of bias in an AI system (statistical bias) in order to counteract other biases.[31] This means that the system's decisions are intended to reflect reality not as it currently is, but as it should be.[32] In such cases it is a human who decides what vision of the world the AI system is to promote. Should it reproduce the world as it is with maximum accuracy based on collected data, or should it be a tool to correct the world's imperfections by taking decisions that have been somehow 'enhanced'?

A system may prove biased in yet another way, when it finds correlations between certain features of the input data that give a simplified picture of reality. System designers and trainers have to decide which data are significant for the system's purposes and which are to be ignored.[33] Moreover, in building a predictive model, an AI system may assign too great a weight (from an anti-discrimination perspective, say) to features – such as race or sex – that should not be decisive or should not be taken into account at all in the making of particular decisions, for instance in making criminological predictions or hiring employees. As a rule, simply removing a given feature from the database used as the system's training set will not solve this problem. The AI system may take account of the feature indirectly,[34] since in individual cases it will often have an influence on other features that are correlated with it (redundant encodings).[35] For example, from a database containing data obtained from individuals' Facebook profiles, but not including information on their

28 See G. Neff and P. Nagy, Talking to Bots: Symbiotic Agency and the Case of Tay, "International Journal of Communication" 2016, no. 10, pp. 4920–4922.

29 D. Danks and A.J. London, Algorithmic Bias, *op. cit.*, p. 3.

30 S. German, E. Bienstock and R. Doursat, Neural Networks and Bias/Variance Dilemma, "Neural Computation" 1992, vol. 4, no. 1, p. 15.

31 D. Danks and A.J. London, Algorithmic Bias, *op. cit.*, p. 3.

32 F. Lattimore et al., Using Artificial Intelligence, *op. cit.*, p. 29.

33 S. Barocas and A.D. Selbst, Big Data's Disparate Impact, "California Law Review" 2016, vol. 104, no. 2, p. 688.

34 D. Roselli, J. Matthews and N. Talagala, Managing Bias in AI, "Companion Proceedings of the 2019 World Wide Web Conference, San Francisco, CA, USA", May 2019, pp. 2–3.

35 E. Ntoutsi, P. Fafalios, U. Gadiraju, V. Iosifidis, W. Nejdl, M.-E. Vidal, S. Ruggieri, F. Turini, S. Papadopoulos, E. Krasanakis, I. Kompatsiaris, K. Kinder-Kurlanda, C. Wagner, F. Karimi, M. Fernandez, H. Alani, B. Berendt, T. Kruegel, C. Heinze, K. Broelemann, G. Kasneci,

sexual orientation, it is possible to predict their orientation relatively accurately by analysing the types of people who appear as their friends.[36]

What is more, in seeking correlations between data, an AI system may ascribe significance to incidental features that are of no importance in practice, but are nonetheless present in the dataset given. This mechanism is well illustrated by an experiment conducted by Ribeiro, Singh and Guestrin concerning the training of an AI system for image recognition. The system was supposed to distinguish photographs of wolves from photographs of husky dogs, which indeed it did with a high degree of accuracy. However, deeper analysis showed that the key criterion being used by the system was not any of the animals' features, but the presence or absence of snow in the photograph. If snow appeared, the system decided the picture was of a wolf; if not, it was deemed to show a dog.[37] Although this accidental correlation did in fact hold true for the collection of photographs used, a wolf is not a wolf merely because there is snow around it.[38]

Paradoxically, the experiment shown above can be used as an argument for utilizing artificial intelligence systems in real life. If the system is found to be biased through assigning inappropriate weight to certain features, then this bias can be detected and the system redesigned or simply retrained to meet relevant criteria. When it comes to decisions made by humans, the detection of bias could be much more complicated, for a seemingly objective substantiation may be backed with deep-seated prejudice, emotions or even certain fixed states, such as time of day or even hunger, felt while making a decision.[39] Taking into consideration the above, humans are much less 'fixable' than AI systems.

Humans themselves may be the source of bias in an AI system. As noted above, it is humans who design and train the system, and in doing so take decisions that will ultimately affect how the system operates. These may concern the selection of training data, the identification and labelling of significant features of the data and the construction of the system itself, including the use of deliberately biased estimators to eliminate other types of bias. It may therefore happen that human decisions are the original cause of the types of bias presented above. However, human involvement is not limited to those developing the system.

T. Tiropanis and S. Staab, Bias in Data-Driven Artificial Intelligence Systems – An Introductory Survey, "WIREs Data Mining Knowledge Discovery" 2020, vol. 10, no. 3, p. 4.

36 See C. Jernigan and B.F. Mistree, Gaydar: Facebook Friendships Expose Sexual Orientation, "First Monday" 2009, vol. 14, no. 10; F. Zuiderveen Borgesius, Discrimination, Artificial Intelligence and Algorithmic Decision-Making, Strasbourg 2018, p. 13.

37 See M.T. Ribeiro, S. Singh and C. Guestrin, "Why Should I Trust You?" Explaining the Predictions of Any Classifier, '22nd ACM SIGKDD International Conference 2016, San Francisco', pp. 8–10, https://www.kdd.org/ kdd2016/papers/files/rfp0573-ribeiroA.pdf (accessed 06.02.2021).

38 D. Roselli, J. Matthews and N. Talagala, Managing Bias, *op. cit.*, p. 4.

39 H. Fry, Hello World, *op. cit.*, p. 103.

AI systems that could be placed in the category 'general artificial intelligence', meaning a system capable of performing any task requiring intellect at a human level or higher, do not currently exist. Existing systems represent 'narrow artificial intelligence' and are designed to serve specific purposes. An AI system providing a virtual chatbot has different tasks than a system controlling a driverless vehicle or making criminological predictions. The fact that an AI system properly performs the tasks for which it was designed does not mean that it can operate with similar accuracy and confidence in other domains. Moreover, even when a system is used for its intended purpose, bias may be introduced if the conditions are different from those anticipated by its designers. This phenomenon is known as *transfer context bias*. For example, an AI system used to control a driverless vehicle designed for a right-hand traffic environment will not function correctly in a situation where the traffic is on the left.[40] This type of bias may also be related to cultural differences between the countries in which an AI system is used (cultural bias).[41]

Some AI systems are designed to play an advisory role, helping humans to take the right decision. These systems, after analysing the input data, present recommendations or suggestions that the user can accept or reject; any erroneous decision is the user's responsibility. An example of such cooperation between humans and AI can be found in medical diagnostics.[42] The AI system can collect and process data – for example, in the form of medical publications or the medical history of large numbers of patients – with the goal of proposing a diagnosis. Assessing the accuracy of the diagnosis and deciding whether to administer a particular treatment will be the responsibility of a human. Nevertheless, problems may arise in practice owing to the temptation to treat such a system as infallible – as a kind of 'moral buffer'[43] apparently shielding from responsibility a user who is incapable of processing such large sets of data or who lacks the time or skills to take a proper decision.[44] Overconfidence in the results output by an AI system may also be due to failure to understand the principle on which it works. In building a predictive model, the system only seeks correlations between data, that is, the co-occurrence of particular features and the directions of dependence. It does not attempt to explain the identified relationships in terms of cause and effect.[45] Of course, the fact that particular features co-occur does not mean that one feature is the cause of the other and does not provide any explanation for the relationship.

40 D. Danks and A.J. London, Algorithmic Bias, *op. cit.*, p. 3.

41 M. Coeckelbergh, AI Ethics, *op. cit.*, pp. 128–129.

42 T. Davenport and R. Kalakota, The Potential for Artificial Intelligence in Healthcare, "Future Healthcare Journal" 2019, vol. 6, no. 2, pp. 95–96.

43 M.L. Cummings, Automation and Accountability in Decision Support System Interface Design, "The Journal of Technology Studies" 2006, vol. 32, no. 1, p. 26.

44 F. Zuiderveen Borgesius, Discrimination, *op. cit.*, p. 8.

45 F. Lattimore et al., Using Artificial Intelligence, *op. cit.*, p. 20.

An AI system presents its output data only with a certain degree of likelihood – it does not offer certainty.[46] Users must be aware of this, as they are usually the final decision-makers (unless the decision is taken fully automatically by the system, as with the calculation of credit scores, for example). Most often, then, it depends on a human being whether a decision proposed by a biased AI system has an actual effect on the lives of the people the decision concerns. Placing excessive trust in the objectivity and infallibility of AI systems may lead to unequal treatment of people in similar situations. This may be a result of bias in the system or in the data, but the decisive role is played by the person who interprets the result the system generates. A clear example is the above-mentioned COMPAS system, which was designed to make criminological predictions and to justify resocialization decisions taken with regard to specific individuals. In practice, however, judges in many American states used the system to determine offenders' sentences.[47]

The possibility cannot be excluded either that people might deliberately provoke an AI system to make biased decisions. The data collected for testing such a system may be manipulated, resulting in a distorted picture of reality (for example, by overrepresenting or underrepresenting certain features or groups). A system can also be designed deliberately to discriminate against individuals with certain features or against entire social groups. Moreover, it might serve as a kind of filter for identifying people with specific characteristics in order to subject them to repression. It is not difficult to imagine a situation in which an autocratic or totalitarian government might use an AI system to seek out people with features or views that deviate from those expected (based on their social media data, for example) so as to take repressive measures against such persons. In this case, however, the system itself may be functioning correctly from a technical standpoint, the problem being the use to which it is put.[48]

3. Eliminating Bias from AI Systems

Bias in AI systems is a complex phenomenon and may result from various causes occurring at different stages of the system's life cycle. This causes significant difficulty in laying down general conditions and standards to enable the reduction of bias. Moreover, not every actual bias will be of a discriminatory nature from a human rights perspective. For example, an AI system used to diagnose lung cancer may assign different weights to the same factors depending on whether they occur in men or women. This is a consequence of the fact that there exist objective differences between the sexes in terms of etiology, pathophysiology, histology, disease

46 A. Yapo and J. Weiss, Ethical Implications, *op. cit.*, p. 5366.
47 J. Angwin et al., Machine Bias, *op. cit.*
48 M.S. Cataleta and A. Cataleta, Artificial Intelligence, *op. cit.*, p. 45.

risk factors, effectiveness of therapy and survival.[49] In certain circumstances it is possible to restrict application of the right to equal treatment and the prohibition of discrimination, provided that this is done for a lawful purpose, in an appropriate form and in accordance with the principle of proportionality.[50] It would appear, then, that a proper approach is to seek appropriate solutions limited to particular types of bias or particular areas in which an AI system might be used.[51] This requires interdisciplinary studies, with the involvement of programmers, lawyers, ethicists and experts in the fields in which AI systems are to be deployed.

Biased decisions taken by AI systems, if acted on, may go against such values as the right to equal treatment and the prohibition of discrimination. Hence, action is being taken to construct certain ethical and legal frameworks to ensure respect for the rights of the individual when AI systems are used. At European Union level, the concept of 'trustworthy artificial intelligence' is being developed. The need to avoid discrimination has been expressed in a number of documents, including the White Paper on Artificial Intelligence,[52] the Ethics Guidelines for Trustworthy AI[53] and a European Parliament resolution on a framework of the ethical aspects of artificial intelligence, robotics and related technologies.[54] In that resolution, the Parliament called on the European Commission, among other things, to draw up political solutions with regard to bias in AI algorithms, pointing out that this problem can cause real harm to individuals and society. The elimination of bias might be served by the introduction of rules on data processing that could be used to counteract unequal treatment and discrimination in certain situations and provide a driving force for equal rights and positive social changes. The European Parliament also proposes that national supervisory authorities should inspect the datasets used in AI systems and that investment should continue to be made in research, analysis, innovations, and cross-border and intersectoral knowledge transfer to allow the development of AI technologies completely free of any type of profiling, unequal treatment or discrimination. It further proposes to provide citizens with effective means of appeal that would guarantee unbiased human verification of any claims relating to breaches of their rights resulting from the use of algorithmic systems.

49 E. Ntoutsi et al., Bias, *op. cit.,* p. 8.

50 P. Hacker, Teaching Fairness, *op. cit.*, p. 1164ff.

51 F. Zuiderveen Borgesius, Discrimination, *op. cit.,* p. 39.

52 White Paper on Artificial Intelligence. A European Approach to Excellence and Trust, COM(2020) 65 final, European Commission, Brussels 2020, p. 22.

53 High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, Brussels 2019, pp. 13, 23.

54 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)).

The actions mentioned above are a part of the 'ecosystem of trust' being built within the EU, where apart from the assurance of equal treatment, consideration is also given to such issues as the right to privacy, the autonomy, transparency and explicability of AI systems, and responsibility for inappropriate system operation.

In the literature on bias in AI systems, it is noted that general principles, although important in indicating directions for action, are difficult to put into practice because of their lack of precision.[55] Combating bias, however, is something that can be approached from two directions. First, it is possible to take preventive measures, aimed at preventing the creation of bias, through appropriate data selection and the 'sanitization' of biased data, and also to ensure that designers (as well as trainers and testers) evaluate system operation not only from a technical but also a social perspective (for example, in accordance with the 'fairness-by-design' concept).[56] This is an extremely difficult task, however, requiring designers to have profound knowledge of the prejudices and inequalities that may be transferred to an AI system, particularly in the case of indirect discrimination, which is often not easy to identify.[57] Moreover, AI systems are often commercial products, and their source code (being a trade secret) is not made public; this is a significant limitation on attempts to analyse a system's bias before it is brought into use.[58] Thus, for this method of eliminating AI system bias to work, it is essential to enforce code transparency.[59] It should also be noted that independent tools are being created to identify algorithmic bias, such as the AI Fairness 360 Open Source Toolkit.[60] Therefore, it seems reasonable to postulate that the design and audit teams of such systems should consist not only of technical experts but also of ethicists and lawyers, especially if those systems could be used in an area connected with the rights and freedoms of an individual. As indicated above, an AI system may be functioning properly from a technical point of view but its use may still result in some negative social consequences. Not everything that is technically possible is at the same time ethically justified.

A second approach uses the possibility of human elucidation and verification of decisions that have been made by the system. This solution is of a corrective nature, enabling the elimination of biased decisions that the system itself has taken. It may

55 E. Ntoutsi et al., Bias, *op. cit.*, p. 9; F. Zuiderveen Borgesius, Discrimination, *op. cit.*, p. 19.

56 See F. Lattimore et al., Using Artificial Intelligence, *op. cit.*, p. 55.

57 B. Berendt and S. Preibusch, Toward Accountable Discrimination-Aware Data Mining: The Importance of Keeping the Human in the Loop – and Under the Looking-Glass, "Big Data" 2017, vol. 5, no. 2, p. 145.

58 I.D. Raji and J. Buolamwini, Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products, "Conference on Artificial Intelligence, Ethics, and Society" 2019, p. 1, https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products/ (accessed 06.02.2021).

59 M.S. Cataleta and A. Cataleta, Artificial Intelligence, *op. cit.*, p. 47.

60 R. Rodrigues, Legal and Human Rights Issues, *op. cit.*, p. 3.

involve assigning to the AI system the role of 'advisor' to a human decision-maker[61] or allowing the system to take its own decisions but with the possibility of appeal to a human assessor. To make verification of the system's decisions possible at all, it must fulfil the requirement of explainability – that is, the possibility of presenting the system's decision-making process in a way that a human can understand.[62]

4. AI Systems as Tools for Reducing Social Inequalities

The right to equal treatment and the non-discrimination approach are expressed nowadays as human rights both in international conventions[63] and constitutions.[64] The essence of the principle of equality is that entities in a similar situation should be treated in a similar way, and entities in a different situation in a different way, respectively.[65] However, this principle is not absolute and does not mean that the rights of all individuals are identical. It should always be related to a certain situational context in order to properly assess a case.[66]

The principle of equal treatment may also be subject to limitations. For example, under Polish law it is acceptable to treat similar entities differently if this is in line with the principle of social justice.[67] Assessment as to whether such a differentiation is justified or not is based on the relevance of the differentiation's character, the proportionality of the arguments for differentiation and the constitutional basis for the differentiation.[68] One example of such a non-discriminatory differentiation is the so-called compensatory privilege, i.e. the one aimed at reducing inequalities actually occurring in social life.[69]

It seems that AI systems could be used as a tool to minimize inequalities due to the fact that those systems may be biased. Firstly, utilizing such systems and subsequent analysis of their decisions may allow revealing of prejudices hidden within the society, which could be exposed using statistical data. Secondly, it could be possible to facilitate the use of estimators to introduce corrective measures to the system (although often, due to the complexity of the situation and the multitude of

61 B. Berendt and S. Preibusch, Toward Accountable, *op. cit.*, p. 146.
62 E. Ntoutsi et al., Bias, *op. cit.*, p. 8.
63 For example, Art. 14 of the Act of 4 November 1950 – Convention for the Protection of Human Rights and Fundamental Freedoms (Journal of Laws 1993, No. 61, item 284).
64 Art. 32 of the Act of 2 April 1997 – The Constitution of the Republic of Poland (Journal of Laws 1997, No. 78, item 483, as amended).
65 W. Borysiak and L. Bosek, Komentarz do art. 32, (in:) M. Safjan and L. Bosek (eds.), Konstytucja RP. Tom I. Komentarz do art. 1–86, Warsaw 2016, p. 831.
66 *Ibidem*, pp. 831–832.
67 Judgement of the Constitutional Tribunal of 24 February 1999, SK 4/98, Lex No. 36177.
68 Judgement of the Constitutional Tribunal of 3 September 1996, K 10/96, Lex No. 25751.
69 Judgement of the Constitutional Tribunal of 28 March 2000, K 27/99, Lex No. 39995.

variables, it may prove to be difficult to implement in practice). Thirdly, it would be possible to design the system to 'reward' certain features as a means to achieve compensatory privilege. In the end, paradoxically, AI systems' bias can be used to remove real social inequalities.

However, some possible problems should be highlighted. The first of these concerns would be who should decide to introduce equalization mechanisms to such a system. Usually AI systems are commercial products made by private entities. Equipping them with such authorization to influence social reality seems too far-reaching, and it seems necessary to introduce mechanisms of cooperation with the state authorities. The problem, however, increases when such a system is to be used solely by the private entity (e.g. for employee recruitment or credit risk assessment). Then the involvement of the state authority in such cases would be limited. What is more, social inequalities existing in one country do not necessarily exist in others, and even if they do, not usually to the same extent. This means that AI systems used to reduce social inequalities would have to take into account the specificity of each country in which they are to be used.

The second problem is to establish a vision of the future reality that would be achieved with these systems. It would require a diagnosis of existing inequalities and the setting up of groups of people or features impacted by those inequalities. The next step would be to determine the appropriate direction of change. In a democratic state ruled by law, it should be established by means of a social consensus based on rational premises. An arbitrarily set direction of change could lead to replacing existing social inequalities with others, e.g. through disproportionately favouring certain groups.

Regardless of whether or not AI systems will be actively used to reduce social inequalities, or whether actions aimed at ensuring equal treatment will be limited to adjusting the decisions of such a system in individual cases, human involvement in the decision-making process seems indispensable. It appears that the limitations of the AI system combined with understanding the context (a human domain) would allow us to make the most of AI capabilities. On the one hand, the bias of AI systems does not in itself prejudge their rejection; on the other hand, these systems do not reduce social inequalities on their own but may be a powerful tool in the hands of a human.

Conclusion

Like any technology, artificial intelligence in itself is neither good nor bad. It is people who impart it such a character when they decide how a system is to be used. AI is used in various areas of human life and sometimes produces spectacular results, for example by improving the diagnosis of cancer. However, we must not lose sight of the fact that AI systems are not a remedy for the stereotypes, nurtured over many

years, that do harm to people with particular characteristics or to whole social groups. These may infect the operation of AI systems in various ways, including the use of biased data, bias resulting from the way the system functions and bias being an effect of the actions of the designer of the system or the person interpreting its decisions. This does not mean that people should stop using artificial intelligence – quite the reverse. It is necessary, however, to be aware of the limitations of such systems and to take measures to overcome those limitations, and also to understand that humans' decisions have a moral character and can affect the operation of the AI systems that they design and use.

It becomes necessary in this regard to take certain difficult decisions about whether we as a society are prepared to allow AI systems to ignore certain data (on race, for instance), accepting a certain reduction in the accuracy of the system's decisions and forecasts, for the sake of ensuring equality, understood as the treatment of similar individuals in similar ways. Another question to be answered is how far it is justified to take steps to eliminate statistical bias through the deliberate introduction of other types of bias into AI systems' operation. Although solutions of this type may reduce the effects of existing prejudices, they are based on a certain predefined vision of the world and may thus serve as a way of designing the future. It is therefore necessary to act with particular vigilance and to ask ourselves, while we still have time, what kind of future world that ought to be.

REFERENCES

Angwin J., Larson J., Mattu S. and Kirchner L., Machine Bias, ProPublica 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Barfield W. and Pagallo U., Advanced Introduction to Law and Artificial Intelligence, Cheltenham/Northampton 2020.

Barocas S. and Selbst A.D., Big Data's disparate impact, "California Law Review" 2016, vol. 104, no. 2.

Berendt B., Preibusch S., Toward accountable discrimination-aware data mining: The importance of keeping human in the loop – and under the looking-glass, "Big Data" 2017, vol. 5, no. 2.

Boden M.A., Sztuczna inteligencja. Jej natura i przyszłość, trans. T. Sieczkowski, Łódź 2020.

Borysiak W. and Bosek L., Komentarz do art. 32, (in:) M. Safjan and L. Bosek (eds.), Konstytucja RP. Tom I. Komentarz do art. 1–86, Warsaw 2016.

Brennan T., Dieterich W. and Ehret B., Evaluating the predictive validity of the COMPAS risk and needs assessment system, "Criminal Justice and Behavior" 2009, vol. 36, no. 1.

Cataleta M.S. and Cataleta A., Artificial Intelligence and Human Rights, an Unequal Struggle, "CIFILE Journal of International Law" 2020, vol. 1, no. 2.

Coeckelbergh M., AI Ethics, Cambridge/London 2020.

Cummings M.L., Automation and Accountability in Decision Support System Interface Design, "The Journal of Technology Studies" 2006, vol. 32, no. 1.

Danks D. and London A.J., Algorithmic Bias in Autonomous Systems, 'Proceedings of the 26th International Joint Conference on Artificial Intelligence (IJCAI 2017)', https://www.cmu.edu/dietrich/philosophy/docs/london/IJCAI17-AlgorithmicBias-Distrib.pdf.

Davenport T. and Kalakota R., The potential for artificial intelligence in healthcare, "Future Healthcare Journal" 2019, vol. 6, no. 2.

Dymitruk M., Sztuczna inteligencja w wymiarze sprawiedliwości? (in:) L. Lai and M. Świerczyński (eds.), Prawo sztucznej inteligencji, Warsaw 2020.

European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)).

Fjeld J., Achten N., Hilligoss H., Nagy A. and Srikumar M., Principled Artificial Intelligence. Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI, Cambridge 2020.

Flasiński M., Wstęp do sztucznej inteligencji, Warsaw 2020.

Fry H., Hello world. Jak być człowiekiem w epoce maszyn, trans. S. Musielak, Krakow 2019.

German S., Bienstock E. and Doursat R., Neural networks and bias/variance dilemma, "Neural Computation" 1992, vol. 4, no. 1.

Hacker P., Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law, "Common Market Law Review" 2018, vol. 55.

High-Level Expert Group on Artificial Intelligence (appointed by the European Commission in June 2018), A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines, Brussels 2019.

High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, Brussels 2019.

Jernigan C. and Mistree B.F., Gaydar: Facebook friendships expose sexual orientation, "First Monday" 2009, vol. 14, no. 10.

Kasperska A., Problemy zastosowania sztucznych sieci neuronalnych w praktyce prawniczej, „Przegląd Prawa Publicznego" 2017, no. 11.

Lattimore F., O'Callaghan S., Paleologos Z., Reid A., Santow E., Sargeant H. and Thomsen A., Using artificial intelligence to make decisions: Addressing the problem of algorithmic bias. Technical Paper, Australian Human Rights Commission, Sydney 2020.

Massey G. and Ehrensberger-Dow M., Machine learning: Implications for translator education, "Lebende Sprachen" 2017, vol. 62, no. 2.

Michie D., Methodologies from Machine Learning in Data Analysis and Software, "The Computer Journal" 1991, vol. 34, no. 6.

Neff G. and Nagy P., Talking to Bots: Symbiotic Agency and the Case of Tay, "International Journal of Communication" 2016, no. 10.

Ntoutsi E., Fafalios P., Gadiraju U., Iosifidis V., Nejdl W., Vidal M.-E., Ruggieri S., Turini F., Papadopoulos S., Krasanakis E., Kompatsiaris I., Kinder-Kurlanda K., Wagner C., Karimi F., Fernandez M., Alani H., Berendt B., Kruegel T., Heinze Ch., Broelemann K., Kasneci G., Tiropanis T. and Staab S., Bias in data-driven artificial intelligence systems – An introductory survey, "WIREs Data Mining Knowledge Discovery" 2020, vol. 10, no. 3.

O'Neil C., Broń matematycznej zagłady. Jak algorytmy zwiększają nierówności i zagrażają demokracji, trans. M. Z. Zieliński, Warsaw 2017.

Raji I.D., Buolamwini J., Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products, 'Conference on Artificial Intelligence, Ethics, and Society' 2019, https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products/.

Ribeiro M.T., Singh S. and Guestrin C., „Why Should I Trust You?" Explaining the Predictions of Any Classifier, "22nd ACM SIGKDD International Conference 2016, San Francisco", https://www.kdd.org/kdd2016/papers/files/rfp0573-ribeiroA.pdf.

Rodrigues R., Legal and human rights issues of AI: Gaps, challenges and vulnerabilities, "Journal of Responsible Technology" 2020, vol. 4.

Roselli D., Matthews J., Talagala N., Managing Bias in AI, "Companion Proceedings of the 2019 World Wide Web Conference, San Francisco, CA, USA", May 2019.

Rutkowski L., Metody i techniki sztucznej inteligencji, Warsaw 2012.

White Paper On Artificial Intelligence. A European approach to excellence and trust, COM(2020) 65 final, European Commission, Brussels 2020.

Yapo A. and Weiss J., Ethical Implications of Bias In Machine Learning, "Proceedings of the Annual Hawaii International Conference on System Sciences" 2018.

Zuiderveen Borgesius F., Discrimination, artificial intelligence and algorithmic decision-making, Council of Europe, Strasbourg 2018.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.03

Received: 1.09.2021
Accepted: 15.09.2021

Dariusz Szostek
University of Silesia, Poland
dariusz.szostek@szostek-bar.pl
ORCID ID: https://orcid.org/0000–0002-8924–6968

Is the Traditional Method of Regulation (the Legislative Act) Sufficient to Regulate Artificial Intelligence, or Should It Also Be Regulated by an Algorithmic Code?

Abstract: The issue of the regulation of artificial intelligence (AI) is one of the significant challenges faced by the EU at present. Most researchers focus on the substantive scope of AI regulation, including state law, ethical norms and soft law. In addition to the substantive and legal scope of the regulation, it is worthwhile considering the manner of such regulation.[1] Since AI is an algorithmic code, it seems correct to regulate (restrict) AI not so much with traditional law established in natural (human) language as with one implemented into algorithms. They may operate as a tool supporting traditional legislation (RegTech), but it is possible to go further with the issue and create regulation algorithms which implement the law as the effective law. However, this requires a new approach to law and legislation – the law as algorithmic code.

Keywords: AI, AI ecosystem, AI regulation, Algorithm, law as IT code, RegTech, LegalTech

1 In an earlier publication, the author referred to smart contracts as a method of regulation: D. Szostek, Sztuczna inteligencja a kody. Czy rozwiązaniem dla uregulowania sztucznej inteligencji jest smart contract i blockchain? (in:) L. Lai and M. Świerczyński (eds.), Prawo Sztucznej Inteligencji, Warsaw 2020, p. 15ff. This article is an extension of the original idea.

Introduction

Both the documents[2] and the statements of science[3] and practice refer to the significance of the development of a digital economy based on artificial intelligence (AI), with simultaneous identification of the risks and dangers related thereto.[4] AI is a challenge to economies, states and contemporary law and the manner of its application.[5] One of the recurring issues in the scientific discussion is artificial intelligence regulation.[6] The question is not only about the issue of the scope of the subject matter of the regulation[7] but also the manner of regulation. The traditional

2 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels (COM(2018) 237), 25.04.2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM% 3A2018%3A237%3AFIN; The High-Level Expert Group on Artificial Intelligence European Commission Directorate-General for Communications Networks Technology, 20.09.2018; Recommendation No. 2102 (2017) about technological convergence, artificial intelligence and human rights (Doc. 14432); Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, 13.02.2019,; European Commission For The Efficiency Of Justice, European Ethical Charter on the use of artificial intelligence in judicial systems, Guidelines on Artificial Intelligence and Data Protection T-PD(2019)01, 14.04.2021,.

3 N.D. Wright (ed.), Artificial Intelligence, China, Russia, and the Global Order, Maxwell 2019, p. 2ff.; S. Feldstein, The Global Expansion and AI Surveillance, Washington 2019, p. 5ff. See also National AI Strategies.

4 Australian Government, Artificial Intelligence: Solving problems, growing the economy and improving our quality of life, 20.12.2019, https://data61.csiro.au/en/Our-Research/Our-Work/AI-Roadmap; Executive Office of the President of the United States, 2016–2019 Progress report: Advancing artificial intelligence R&D (November 2019), https://www.whitehouse.gov/wp-content/uploads/2019/11/AI-Research-and-Development-Progress-Report-2016–2019.pdf (accessed 09.04.2021); National Artificial Intelligence Strategy of the Czech Republic, https://www.mpo.cz/assets/en/guidepost/for-the-media/press-releases/2019/5/NAIS_eng_web.pdf (accessed 14.04.2021); EU guidelines on ethics in artificial intelligence: Context and implementation, https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf (accessed 31.03.2021); Responsibility and AI: Council of Europe study, 21.12.2019, https://rm.coe.int/responsability-and-ai-en/168097d9c5.

5 European Artificial Intelligence (AI) leadership, the path for an integrated vision https://nws.eurocities.eu/MediaShell/media/European_AI_study.pdf (accessed 20.04.2021).

6 White Paper On Artificial Intelligence. A European approach to excellence and trust, COM(2020) 65 final, European Commission, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (19.04.2019).

7 I suggest reading interesting recommendations concerning liability issued by EU experts: Liability for Artificial Intelligence and other emerging digital technologies: Report from the Expert Group on Liability and New Technologies – New Technologies Formation, https://ec.europa.eu/transparency/regexpert/index.cfm?do= groupDetail.groupMeetingDoc&docid=36608 (accessed 12.04.2021).

method of AI regulation is necessary but seems to be insufficient.[8] Increasingly often, modern law applies the tools of LegalTech[9] and RegTech[10] to support the processes of the analysis or application and even enforcement of law.[11] In reality, regulating AI only with the text of a legal act is so complicated that it is very difficult, if not impossible, to reach it through a traditional way of lawmaking. At the most, it may be a way of imposing rights and obligations that will have to be taken into account on the entities teaching or using AI in the process of AI coding or teaching, and thus finally effecting the transformation of law into codes.

Therefore, it is necessary to formulate the following hypothesis: Since AI is an algorithm, then the method of its regulation should be the use of an algorithm comprising legal standards. The question is, Should such an algorithm be a RegTech tool supporting traditional legislation, or should it be the law incorporated into the code? Who should create and enforce such algorithms? Should it remain the domain of private entities that use or teach AI, or the domain of states or maybe of the European Union? And who is to control the AI-regulating algorithms and ensure their cybersecurity?

It is not possible to include all the regulation aspects of AI in such a short publication. The issue requires separate and in-depth scientific research and a separate monograph.[12] The goal of this article is to prove that the hypothesis formulated above is correct and to answer the above questions. At the least, the article is just a contribution to the discussion of AI regulation. The author deliberately passes over the issue of the substantive layer[13] of AI regulation and concentrates on the

8 https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608 (accessed 20.04.2021).

9 The goal of this article is not the analysis of the definition of LegalTech or RegTech. For more, see M. Hartung, M. Bues and G. Halblieb, Legal Tech, Baden-Baden 2018, p. 11ff.

10 Compare the issue of the term and application of RegTech in T. Kerikmäe (ed.) Regulating eTechnologies in the European Union. Normative Realities and Trends, Cham 2014, p. 7ff. See also Recommendations on regulation, innovation and finance: Final Report to the European Commission, 01.12.2019, p. 27ff., https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf. The analysis of the scope of the terms of LegalTech and RegTech exceeds the scope of this article.

11 R. Leens, Regulating New Technologies in Times of Change, (in:) L. Reins (ed.), Regulating New Technologies in Uncertain Times, Cham 2019, pp. 3–19; D. Szostek (ed.), Legal Tech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym, Warsaw 2021, p. 3ff.

12 See: D.E. Harasimiuk and T. Braun, Regulating Artificial Intelligence. Binary Ethics and the Law, London/ New York 2021, p. 1ff.

13 Compare: On factual regulation: Documents of the European Commission, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf; M. Chinen, Law and Autonomous Machines, Cheltenham 2019, p. 2ff.; J. Turner, Robot Rules. Regulating Artificial Intelligence, Cham 2019, p. 133ff., where the author specifies different law aspects

analysis of whether it is sufficient for the correct AI regulation to have traditional legal provisions created and published in a natural language or whether an algorithm should be applied (we can call it the regulation algorithm) which implements the said provisions within its scope. If so, then whoever creates and controls it, and whether it should be something like a RegTech tool supporting traditional regulation or whether as code, it should become the effective law.

The terms AI, codes or algorithms bring a lot of doubt in the scholarship, deepened by the European Commission's proposed Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain union legislative acts (the AI Act),[14] where (in the annexe) AI is very broadly defined to include not only self-learning algorithms, but, more broadly, expert systems as well. International legal scholarship distinguishes three types of AI – algorithms, expert systems and machine learning.[15] This concept is highly underdefined, as is the definition of an algorithm, which can take various forms. It also has no uniform definition.[16] The problem of definition alone is very broad and lends itself to separate studies much broader than the framework of a single article. The aim of this publication is the question of the method of regulation and not its scope or the solution of definition problems. Therefore, for its purposes, some simplifications are assumed without going into conceptual issues.[17] The following considerations concern the so-called self-learning algorithms (for the purposes of this article included under the general term AI).

for AI, both orders and prohibitions in relation to human rights or individual law systems, but also thinks of the law only and exclusively for AI, similar to how we have rights for animals. Examples of material solutions are: Report with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), https://www.europarl.europa.eu/doceo/document/A-9–2020-0178_EN.html (accessed 20.04.2021); Artificial Intelligence (AI): new developments and innovations applied to e-commerce, https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2020)648791 (accessed 20.04.2021).

14 Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts Com/2021/206 Final, https://Eur-Lex.Europa.Eu/Legal-Content/EN/TXT/?Uri=CELEX:52021PC0206 (accessed 19.07.2021).

15 W. Barfield and U. Pagallo, Law and AI, Cheltenham/Northampton 2020, pp. 19–23; R. Prabucki, D. Szostek and J. Wyczik, Prawo jako kod, (in:) D. Szostek (ed.), Legal Tech, *op. cit.*, p. 21.

16 *Ibidem*, p. 17ff., and the literature cited therein.

17 In Polish scholarship, compare: A. Krasuski, Status sztucznego agenta. Podstawy prawne zastosowania sztucznej inteligencji, Warsaw 2021, p. 3 ff.; L. Lai and M. Świerczyński (eds.), Prawo Sztucznej Inteligencji, *op. cit.*, p. 1ff.

1. Incorporation of Law into Codes

Artificial intelligence is a specific algorithm which may itself take decisions independently and 'learns' in closed or open ecosystems.[18] AI is characterised by variability, activity and the ability to interpret the collected structured or unstructured data, to draw conclusions from the knowledge obtained from data and to select the best actions to achieve the goal. In other words, AI is able to learn.[19] The regulation concerning restrictions for AI should take this characteristic into account. In other words, while learning, AI should take into account the restrictions (that is, the law) imposed on it.[20] AI does not have any possibility to consider the restrictions of law published in natural language in traditional legislation. Yet it would be possible if the law concerning AI was implemented into algorithmic codes.[21]

L. Lessig's concept[22] that code is law and the legal system is composed of 'puzzles' which can be combined with one another and formed in cyberspace, among others, has become the reality nowadays. It is no longer a theoretical concept but has the form of actually implemented projects where the human language – used thus far to notify the legal rules to be observed by the society – is replaced with the programming codes readable by machines equipped with processors and directly

18 More about the definition and characteristics of AI can be found in J. McCarthy, M. L. Minsky, N. Rochester and C.E. Shannon, A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf (accessed 20.04.2021): 'every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it'; A. Turing, Computing Machinery and Intelligence, "Mind" 1950, vol. 49, no. 236, p. 433, https://www.cse-e.umbc.edu/courses/471/papers/turing.pdf (accessed 20.04.2021); Collins Dictionary: "Artificial intelligence is a type of computer technology which is concerned with making machines work in an intelligent way, similar to the way that the human mind works"; Merriam-Webster Dictionary: "the capability of a machine to imitate intelligent human behaviour"; Communication from the Commission, *op. cit.*; HLEG AI Definition 2018: The European Commission's high-level expert group on artificial intelligence, A definition of AI: Main capabilities and scientific disciplines. Definition developed for the purpose of the deliverables of the High-Level Expert Group on AI, Brussels, 18.12.2018, https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines. See also the definition from May 2019 in the Recommendation of the Council on Artificial Intelligence, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

19 For more, see: T. Zalewski, Definicja sztucznej inteligencji, (in:) L. Lai and M. Swierczyński (eds.), Prawo Sztucznej Inteligencji, *op. cit.*, pp. 11–12.

20 For more about AI learning, see: M. Tegmark, Życie 3.0. Człowiek w Erze sztucznej Inteligencji, Warsaw 2019, p. 111ff.

21 This is not the first such postulation in scholarship. In 2018, such a need was pointed out by K. Werbach, in The Blockchain and the New Architecture of Trust, London 2018, pp. 1–7.

22 L. Lessig, Code and Other Laws of Cyberspace, New York 1999, p. 3ff.

executed by them.[23] Such a process is carried out without the transcription of a computer code into symbols, letters, words, phrases and sentences, in a manner that cannot be directly perceived by humans.[24] A legal provision or a contract starts to operate as a computer program and not as a text including legal provisions composed of letters and grammatical characters presented in natural language.[25] Law and technology interact[26] with each other increasingly intensively through a complex system of relations and correlations, as both of them contribute to the regulation of the behaviour of entities such as individuals, where the law regulates such behaviour as the system of orders and prohibitions, while the programming codes regulate the actual restrictions[27] on the freedom of those who use it in cyberspace.[28] Thus far, the codes have mainly restricted the freedom of people operating in cyberspace. Why can they not restrict other codes, such as AI? Code is the architecture of cyberspace, and pieces of code are the construction material of such architecture. Everything we see online is delivered through a code; only a code can allow the presence of social rules in cyberspace. Thus, the code also functions as a regulator.[29]

The functions of codes in cyberspace are described in a similar manner by Lessig. He claims that cyberspace is not entirely a zone of full liberty but is regulated. The author states that 'This regulator is code – the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general

23 See: M. Araszkiewicz, Algorytmizacja myślenia prawniczego. Model, możliwości ograniczenia, (in:) D. Szostek (ed.), Legal Tech, *op. cit.*, p. 55ff.

24 Attention was drawn to it in the literature as early as 2002; see: A. Wiebe, Die elektronische Willenserklärung, Tubingen 2002, p. 350; D. Szostek, Czynność prawna a środki komunikacji elektronicznej, Krakow 2004, p. 39. See also: W. Cyrul, LegalTech a tworzenie i publikacja tekstów prawnych, (in:) D. Szostek (ed.), Legal Tech, *op. cit.*, p. 88ff.

25 More on the transcription of spoken language into algorithmic codes is in: M. Araszkiewicz, Algorytmizacja, *op. cit.*, p. 55.

26 An example includes the analysis of the correct implementation of 42 directives in Ireland, Luxembourg and Italy performed by an expert system; see: R. Nanda, G. Siragusa, L. Di Caro, G. Boella, L. Grossio, M. Gerbaudo and F. Costamanga, Unsupervised and Supervised Text Similarity Systems for Automated Identification of National Implementing Measures of European Directives, "Artificial Intelligence and Law" 2019, vol. 27, p. 1999ff. Also see: R. Boulet, P. Mazzega and D. Bourcier, Network Approach to the French System of Legal Codes, part II: The Role of the Weights in a Network, "Artificial Intelligence and Law" 2018, vol. 26, p. 23ff.

27 The transformation of law into programming codes is a new scientific discipline which combines law and computer science and thus creates so-called LegalTech. See: S. Schrebak, Integrating Computer Science into Legal Discipline: The Rise of Legal Programming, pp. 1–33, https://papers.ssrn.com/sol3/papers.cfm? abstract_id=2496094 (accessed 22.09.2019); M. Corrales, M. Fenwick and H. Haapio, Legal Tech, Smart Contracts and Blockchain, Singapore 2019, p. 5ff.

28 W. Szpringer, Blockchain jako innowacja systemowa. Od Internetu informacji do Internetu wartości, Warsaw 2018, p. 40.

29 S. Schrebak, Integrating Computer Science, *op. cit.*, p. 4.

or whether information is zoned. It affects who sees what, or what is monitored and invisible. Code regulates cyberspace in ways that one cannot begin to see unless one begins to understand the nature of this code. The code of cyberspace is changing. And as this code changes, the character of cyberspace will change as well.'[30] G. Wood puts it similarly in his work, indicating that cryptography makes it possible to implement law into codes. In the terms of his concept, crypto-law is characterised by the fact that it is possible to implement legal rules known from traditional law into codes in a highly secured cryptographic space. The moment when this became possible is the development of blockchain technology.[31] A similar possibility is indicated by M. Hildebrand, who asks to what extent algorithmic regulation could replace or support legal regulation.[32]

Cyberspace is an artificial creation operating through software.[33] AI is an algorithmic code constituting an element of cyberspace, and therefore it could be regulated through the same technique, that is, through the codes with legal regulations implemented into them. Cyberspace is dynamic and undergoes continuous changes. AI is also dynamic and undergoes continuous changes, and therefore the method of regulation should also be subject to dynamism,[34] to appropriately adapt to changing social relations[35] and take into account different spaces and legal systems. In other words, the process of AI teaching or AI learning should take into account the legal restrictions imposed on it, which may be achieved either through appropriately created data ecosystems or through appropriate algorithms with legal regulations (restrictions) for AI implemented into them.

30 L. Lessig, Code is Law: On Liberty in Cyberspace, "Harvard Magazine", https://harvardmagazine.com/2000/ 01/code-is-law-html (accessed 19.04.2021).

31 G. Wood, Ethereum: A Secure Decentralized Generalized Transaction Ledger (EIP-150 revision), http://gavwood.com/Paper.pdf (accessed 19.07.2021), See: also R. Prabucki, D. Szostek and J. Wyczik, Prawo jako kod, *op. cit.*, p. 23; Compare M. Hildebrandt, Smart Technologies and the End(s) of Law, Northampton 2016, p. 1ff.

32 M. Hildebrandt, Algorithmic Regulation and the Rule of Law, 'Philosophical Transactions of the Royal Society A' 2018, vol. 376, issue 2128, https://royalsocietypublishing.org/doi/10.1098/rsta.2017.0355 (accessed 19.07.2021).

33 L. Lessig, Code and Other Laws, *op. cit.*, p. 82.

34 M. Fenwick, E.P.M. Vermeulen and M. Corrales, Business and Regulatory Responses to Artificial Intelligence: Dynamic Regulation, Innovation Ecosystems and the Strategic Management of Disruptive Technology, (in:) M. Corrales, M. Fenwick and Nikolaus Forgó (eds.), Robotics, AI and the Future of Law, Singapore 2018, p. 88.

35 Compare J.P. Aires, D. Pinheiro, V. Strube de Lima and F. Meneguzzi, Norm Conflict Identification in Contracts, "Artificial Intelligence and Law" 2017, vol. 25, p. 397ff.

2. Algorithms as an AI Regulation Tool?

The dynamism[36] of AI regulation cannot be correctly dealt with only by traditional legislation published in a natural language. Yet a regulation algorithm may facilitate it. Pursuant to the guidelines included in 'A White Paper on Artificial Intelligence – A European approach to excellence and trust' (COM(2020) 65 final) and also with the AI Act, AI should be characterised by transparency and accountability, and a solid regulatory framework protects EU citizens and helps create the European market for AI.[37] The regulation algorithm may constitute a relevant tool which guarantees transparency, accountability and appropriate dynamism.

The basic feature which distinguishes AI from other algorithms is its possibility to learn by itself in a rational manner.[38] AI systems can be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions.[39] Therefore, there are no obstacles to AI learning the imposed rules, orders and prohibitions which are basic paradigms for it, implemented into algorithmic codes[40] which have been earlier prepared by humans.

---

36 M. Fenwick, E.P.M. Vermeulen and M. Corrales, Business and Regulatory Responses, *op. cit.*, p. 88.

37 It is worth noting the report of Prof. C.H. Wendehorst prepared for the European Commission: Safety and Liability Related Aspect of Software (June 2021), which points to a broader need for algorithmic regulation, not only in the AI Act; https://digital-strategy.ec.europa.eu/en/library/study-safety-and-liability-related-aspects-software (accessed 20.07.2021). For more about this and the substantive scope of the legislation, see: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed 09.04.2021).

38 Definition based on the concept by Marvin Minsky, an AI pioneer, in Perceptrons: M. Minsky, Perceptrons: An Introduction to Computational Geometry, Massachusetts 1969, p. 7ff. See also his: M. Minsky, The Emotion Machine. Commonsense Thinking, Artificial Intelligence, and the Future of the Human Mind, New York/London/Toronto/Sydney 2007, p. 6ff.; M. Yao, M. Jia and A. Zhou, Applied Artificial Intelligence. A Handbook for Business Leaders, Middletown 2018, p. 8; S. Finlay, Artificial Intelligence and Machine Learning for Business, Great Britain 2018, pp. 6–28.

39 Compare other reports: Centre for Information Policy Leadership, Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice. First Report: Artificial Intelligence and Data Protection in Tension, 01.11.2018, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf (accessed 06.02.2019); Interpol Innovation Centre, Singapore, Innovation Report Artificial Intelligence, https://media.licdn.com/dms/document/C4E1FAQHbu EqCSHEUsQ/feedshare-document-pdf-analyzed/0?e=1549350000&v=beta&t=lpYHjU3SizFf82swBk3g33TLFqWGRy8EjbKyhLPsST0 (accessed 07.04.2021).

40 G. Governatori, F. Idelberger, Z. Milosevic, R. Riveret, G. Sartor and X. Xu, On Legal Contracts, Imperative and Declarative Smart Contracts, and Blockchain Systems, "Artificial Intelligence and Law" 2018, vol. 26, p. 398. The authors name a smart contract as a law-regulating tool. In view of this article, the author refers – in a broader manner – not so much to the very notion of a smart contract as to the algorithm that creates it.

The creation of a correctly operating regulation algorithm, or many such algorithms, requires the identification of functional interactions between different elements, and as they change depending on the context,[41] it becomes necessary to create the environment allowing for the measurement of the system's performance.[42] The development of a regulation algorithm requires the information which enables algorithms to make conscious decisions (prohibitions and orders). The quality of the provided information should be measured by such attributes as whether the information is essential, appropriate, understandable, searchable and well-archived. Such indicators are not easily quantifiable, but they are very significant.[43]

The regulation algorithm may be constructed on the data recorded in the available repositories based – for example – on blockchain,[44] which would ensure the reliability of recording and its unchangeability, and thus transparency and accountability,[45] and in practice, the proof that the data transferred to AI is correct. What is important is that blockchain technology has already become very well known and has been well described, and in relation to which legal regulations have been implemented in many countries, of which the legal presumptions of the truth of the facts is recorded in blockchain. In the eIDADS 2 project, the European Commission proposes to link the legal presumption to the entry of data in a qualified electronic register maintained by a qualified certification service provider[46] (which could be a blockchain). This is not an isolated idea. Individual countries are introducing this type of solution, and the EU proposal is more like trying to catch up. Appropriate adjustments include the proceedings to take evidence concerning the data recorded in blockchain, as well as (for example in Malta, New York state and Singapore) the implementation of regulations concerning the control of codes and systems based on blockchain,[47] which may be easily expanded to cover the control of AI.

Both input and output data should be readable (perceptible) by human beings (in spite of the fact that the algorithmic regulator should be recognisable first of all by AI), which – in compliance with the experts' guidelines – would enable the control of the AI teaching or self-learning process. The repository layer should be composed of codified templates, clauses and libraries which should be accessible by AI through

41 Compare *ibidem*, p. 394ff.

42 The possibility of utilising regulatory sandboxes is indicated by M. Fenwick, E.P.M. Vermeulen and M. Corrales, Business and Regulatory Responses, *op. cit.*, p. 89.

43 T.D. Barton, H. Haapio, S. Passera and J.G. Hazard, Successful Contracts: Integrating Design and Technology, (in:) M. Corrales, M. Fenwick and N. Forgó (eds.), Robotics, *op. cit.*, p. 77ff.

44 K. Werbach, The Blockchain and the New Architecture of Trust, *op. cit.*, pp. 1–7.

45 M. Hildebrandt, Algorithmic Regulation, *op. cit.*, *passim*.

46 eIDAS Regulation, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (accessed 15.07.2021).

47 For more, see: D. Szostek, Blockchain and Law, Baden-Baden 2019, p. 5ff. and the literature specified therein.

an interface but – at the same time – possible to be submitted to experts (humans) for their verification or control, also in the form of the text in natural language.[48]

3. Legislator or Private Entity as AI Regulation Algorithm Creator?

Although the concepts for creating a uniform and autonomous law for cyberspace[49] have been suggested for a number of years, their implementation seems to be distant, in spite of the fact that it would significantly facilitate AI regulation. The concept of a separate law for cyberspace is mainly focused on the elimination of the doubts concerning jurisdiction and governing law, as well as the distribution and flow of goods in the digital world.[50] There are different suggestions – from viewing cyberspace as an international space,[51] through cyberspace, as an exterritorial area, being the shared property of all states, to the so-called *lex electronica*.[52] At present, none of these concepts seems to be possible to implement. Therefore, a regulator based on algorithmic code currently seems to be the most viable solution, all the more so because it can operate at different legislation levels, as well as being able to be created both by public and government bodies and by private entities (as a LegalTech). It can also be connected with a specific territory (e.g. the EU, individual states).

Having accepted and taken into account the guidelines of the 'White Paper for AI', software providers will have to create relevant data ecosystems or private regulation algorithms which are subject to ex-post control in case of damage caused by AI.[53] However, a question arises about whether private entities should be the only ones that should create such systems or regulation algorithms. Is it not worthwhile thinking about – when the opportunity arises in connection with AI regulation – the broader implementation of law into algorithmic codes at the level of the European Community and individual Member States? Should the EU legislator limit only the

48 M. Araszkiewicz, Algorytmizacja, *op. cit.*, p. 55ff.; W. Cyrul, LegalTech, *op. cit.*, p. 88ff.

49 Such a concept is supported by D.R. Johnson and D. Post, Law and Borders: The Rise of Law in Cyberspace, 'Stanford Law Review' 1996, vol. 48, no. 5.

50 J. Kulesza, Międzynarodowe prawo Internetu, Poznań 2010, p. 291.

51 D.C. Menthe, Jurisdiction in Cyberspace: A Theory of International Spaces, 'Michigan Telecommunications and Technology Law Review' 1998, no. 69, pp. 69–103.

52 P. Trudel, La lex electronica, (in:) C.A. Morand (ed.), Le droit saisi par la mondialisation, Brussels 2001, p. 221; V. Gautrais, Lex Electronica: d'aujourd'hiu a demain, 'Lex Electronica' 2016, http://www.lex-electronica.org/articles/volume-21/lex-electronica-daujourdhui-a-demain/ (accessed 21.07.2019). The issue of *lex electronica* is also discussed by L. Railas in The Rise of the Lex Electronica and the International Sale of Goods, Helsinki 2004, p. 500ff.

53 Attention should be paid to the suggestion included in 'A White Paper for AI' concerning the requirements for said application.

regulations created and published in a natural language, with the use of RegTech[54] tools as a technological support for traditional regulation at the most?

In the author's opinion, the issue of AI regulation is an excellent opportunity to use RegTech in the legislative process of the European Union, and even further, to establish law implemented into algorithm. The introduction of regulation algorithms for AI at the level of the Community, and created by the Community as the obligatory law, will contribute to the development of AI in the EU, and thus to the cybereconomy. It will be an element supporting small and medium-sized enterprises which – unlike big enterprises – cannot afford costly regulation algorithms. It would also decrease expenditure – once created, a regulation algorithm would be used by many enterprises and other entities of the European Union. It will also contribute to the unification of regulation throughout the Community, and thus the reliability of law. Legislation published only in natural language will not provide such benefits. What is important is that it is not necessary to create the entire legal system in codes for AI at once. It could be started with the creation of legislative 'puzzles' referring to individual spheres which are then slowly interconnected, both horizontally (that is, as individual regulation algorithms of different branches of EU law) and vertically (EU law, national law, local law, etc.).

The current discipline of law shows the territorial, personal and temporary scope of the application of legal provisions. AI regulation algorithms under the legal system implemented into codes may take into account those scopes being the same external source of regulation[55] for AI ecosystems. For just as humans have to observe the provisions according to their hierarchy or the territory of their applicability, it is possible to similarly develop an algorithmic regulator taking into account the nature of such provisions. To put it in different words, the AI regulation should be of a cascading nature.

In the author's opinion, the adoption and implementation of an international convention[56] referring to artificial intelligence is required, which would become the grounds for implementing a technologised code-based AI operator and for introducing such restricting codes,[57] and enforcing consideration of the AI regulator

54 More on the conceptual scope of LegalTech, RegTech and others is in: D. Szostek (ed.), Legal Tech, *op. cit.*, pp. 7–9.

55 It is one of the elements of the divisions of smart contracts. D. Szostek, Blockchain and Law, *op. cit.*, p. 122.

56 Activities concerning the creation of such a convention have been undertaken by the Council of Europe, yet it will take time to achieve results.

57 The discussion of AI regulation refers – quite seriously – to Asimov's Robotics Laws as the elements of such regulation: 1. A robot may not injure a human or, through inaction, allow a human to come to harm; 2. A robot must obey the orders given to it by humans except where such orders would conflict with the First Law; 3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws. The First Law is the answer in the discussion concerning AI and wartime law.

in AI ecosystems. It should be assumed that a convention will be concluded and published in natural language in compliance with the requirements of public international law.

Regardless of the international convention, the European Union is preparing its own EU legislation in natural language, which regulates AI.[58] It is worthwhile thinking about the parallel preparation of the algorithm; depending on the will of the EU, it could take different forms. The optimum solution would be that such an algorithm is the effective law and not only a technological tool supporting the regulation (RegTech). Yet it would require significant changes in the understanding of EU law and legislation. However, it would contribute to the unification of restrictions for AI and the reliability of law in the territory of the EU. The last level should include the national regulation algorithms under the scope of local legislation as a supplement to the EU regulator. This would be a major step into the future and would influence the development of the European digital economy.

Such a process would require the commitment of numerous entities on different levels and with significant outlays, but is possible to implement. However, it requires a different perception of law. A lawyer gains education which enables them to find their way through an impenetrable maze of regulations through many years of work (studies and then legal training). An algorithm would have to be educated in a similar way. Thus the creation of a regulatory system based on algorithms will be very complex, costly and time consuming during the first stage. With time, such a system should become increasingly effective and less costly. It can be started with small sections of law and gradually expanded. The AI regulation is a good opportunity to make such an effort, at the level of both scientific research and implementation. Another solution is to create a single Community RegTech tool (as an integral part of the AI Act) to support AI auditability, especially since, according to the AI Act proposal, there are going to be entities auditing and certifying algorithms at national levels anyway, or as private entities, which will have to create appropriate technological tools (and thus RegTech) to meet the requirements of the proposed act. Instead of multiple, dispersed algorithms, used by a number of different entities, including private ones, when auditing AI, how about a single community tool?

4. Yet It Is Not That Simple

The concept of algorithmic code as an AI regulator presented above may seem futuristic. Yet given the fact that, at present, many activities are concluded and enforced with the use of smart contracts, with complex agreements, and of which some have already been supported by AI or machine learning-based algorithms, may

58 These include the above-mentioned AI Act.

it be that it is still possible to implement such a concept? The algorithm perfectly regulates private law (agreements and smart contracts), so why should it not be expanded to legislation?[59] However, many questions and doubts arise,[60] and also issues requiring further research.

Firstly, how can the entities utilising AI be obligated to connect their ecosystems to the regulation algorithm? How should such a system be developed? What paradigms should be assumed for AI? Which norms and rules should be taken into account? Only the international ones, or also local, imperative or dispositive ones? How should competition and freedom of economic activity be guaranteed? There are issues such as the assessment of values such as liberalism and freedom in cyberspace, and the regulations restricting them; differences in legal systems and cultural differences; ethical issues and their diversification in different cultures; whether the law of nature, ethics, and moral law should be taken into account;[61] the issue of identification of entities on the Internet;[62] the issue of identification of legal systems applicable to a given act (AI and private international law); whether and to what extent precedents and soft law should be taken into account and weighted; whether soft law such as ISO standards and others should be included; who should control the system, in what ways, and what the consequences of violation should be; how to prevent cyberattacks; who should control code and those who write codes, how, and who should control the controllers; what should happen when a law is violated or codes are changed. Such questions may proliferate.[63]

Conclusion

This article is just a contribution to the discussion, focused not so much on the scope as on the technical manner of artificial intelligence regulation. In the author's opinion, when the opportunity arises in connection with AI regulation, it is worthwhile tackling the new perspective on legislation, as law implemented into code (algorithm) but also enforced by algorithm. It seems that the hypothesis concerning AI regulation through regulation algorithms is justified as to its substance and – significantly – as to practice. However, it requires a change of approach to law

59 Such scientific attempts are already being made; see: M. Araszkiewicz, Algorytmizacja, *op. cit.*, p. 55.

60 The issue of difficulties with the utilisation of databases in expert systems is dealt with in M. Badiul Islam and G. Governatori, RuleRS: A Rule-Based Architecture for Decision Support Systems, 'Artificial Intelligence and Law' 2018, vol. 26, p. 7.

61 C. Magnusson Sjöberg, Legal Automation, AI and Law Revisited, (in:) M. Corrales, M. Fenwick and H. Haapio, Legal Tech, *op. cit.*, p. 172.

62 L. Lessig, Code and, *op. cit.*, p. 30, 54.

63 An attempt to answer some of these questions may be found in . Turner, Robot Rules, *op. cit.*, p. 133ff.

and the tradition related thereto. We should consider negatively the concept of the exclusivity of an algorithm as the regulator, without the possibility of verification of law in natural language. Both input and output data should be subject to control by a human being in a manner which is at least indirect (the transcription of codes into natural language), which is in compliance with the AI Act. In other words, the regulation algorithm should operate as a hybrid of the code with the possibility of transcription into natural language. In the author's opinion, the regulation algorithm should be the law and not only a LegalTech tool supporting the regulations, created but mainly published as law by relevant authorities of the EU. This vision is bold, yet not impossible. As a final option, it could be a unified community RegTech tool.

We have a chance for the solution to provide an opportunity for the development of the cybereconomy and greater efficiency. It is worthwhile starting discussion in that regard and to continue scientific research. At the moment, talks and research on an AI regulatory algorithm for Polish state systems are already conducted at the national level in the NASK. Similar work is conducted by other EU countries. In order for this work not to be duplicated, it is worth transferring it to the level of the whole EU.

REFERENCES

Aires J., Pinheiro D., Strube de Lima V. and Meneguzzi F., Norm conflict identification in contracts, "Artificial Intelligence and Law" 2017, vol. 25.

Araszkiewicz M.: Algorytmizacja myślenia prawniczego. Modele, możliwości, ograniczenia, (in:) D. Szostek (ed.), Legal tech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym, Warsaw 2021.

Artificial Intelligence (AI): new developments and innovations applied to e-commerce, https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2020)648791.

Artificial Intelligence and Data Protection in Tension, 01.11.2018, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf.

Australian Government, Artificial Intelligence: Solving problems, growing the economy and improving our quality of life, 20.12.2019, https://data61.csiro.au/en/Our-Research/Our-Work/AI-Roadmap.

Badiul Islam M. and Governatori G., RuleRS: A Rule-Based Architecture for Decision Support Systems, "Artificial Intelligence and Law" 2018, vol. 26.

Barfield W. and Pagallo U., Law and AI, Cheltenham/Northampton 2020.

Barton T.D., Haapio H., Passera S. and Hazard J.G., Successful Contracts: Integrating Design and Technology, (in:) M. Corrales, M. Fenwick and N. Forgó (eds.), Robotics, AI and the Future of Law, Singapore 2018.

Boulet R., Mazzega P. and Bourcier D., Network Approach to the French System of Legal Codes, part II: The Role of the Weights in a Network, "Artificial Intelligence and Law" 2018, vol. 26.

Chinen M., Law and Autonomous Machines, Cheltenham 2019.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels (COM(2018) 237), 25.04.2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM% 3A2018%3A237%3AFIN.

Corrales M., Fenwick M. and Haapio H., Legal Tech, Smart Contracts and Blockchain, Singapore 2019.

Cyrul W., LegalTech a tworzenie i publikacja tekstów prawnych, (in:) D. Szostek (ed.), Legal Tech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym, Warsaw 2021.

Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, 13.02.2019.

eIDAS Regulation, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

EU guidelines on ethics in artificial intelligence: Context and implementation, https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf.

European Artificial Intelligence (AI) leadership, the path for an integrated vision https://nws.eurocities.eu/MediaShell/media/European_AI_study.pdf.

European Commission For The Efficiency Of Justice, European Ethical Charter on the use of artificial intelligence in judicial systems, Guidelines on Artificial Intelligence and Data Protection T-PD(2019)01, 14.04.2021.

Executive Office of the President of the United States, 2016–2019 Progress report: Advancing artificial intelligence R&D (November 2019), https://www.whitehouse.gov/wp-content/uploads/2019/11/AI-Research-and-Development-Progress-Report-2016–2019.pdf.

Feldstein S., The Global Expansion and AI Surveillance, Washington 2019.

Fenwick M., Vermeulen E.P.M. and Corrales M., Business and Regulatory Responses to Artificial Intelligence: Dynamic Regulation, Innovation Ecosystems and the Strategic Management of Disruptive Technology, (in:) M. Corrales, M. Fenwick and Nikolaus Forgó (eds.), Robotics, AI and the Future of Law, Singapore 2018.

Finlay S., Artificial Intelligence and Machine Learning for Business, Great Britain 2018.

Gautrais V., Lex Electronica: d'aujourd'hiu a demain, "Lex Electronica" 2016, http://www.lex-electronica.org/articles/volume-21/lex-electronica-daujourdhui-a-demain.

Governatori G., Idelberger F., Milosevic Z., Riveret R., Sartor G. and Xu X., On legal contracts, imperative and declarative smart contracts, and blockchain system, "Artificial Intelligence and Law" 2018, vol. 26.

Harasimiuk D. E. and Braun T., Regulating Artificial Intelligence. Binary Ethics and the law, London/New York 2021.

Hartung M., Bues M. and Halblieb G., Legal Tech, Baden-Baden 2018.

Hildebrandt M., Smart Technologies and the End(s) of Law, Northampton 2016.

Interpol Innovation Centre, Singapore, Innovation Report Artificial Intelligence, https://media.licdn.com/dms/document/C4E1FAQHbu EqCSHEUsQ/feedshare-document-pdf-analyzed/0?e=1549350000&v=beta&t=lpYHjU3SizFf82swBk3g33TLFqWGRy8EjbKyhLPsST0.

Johnson D. R. and Post D., Law And Borders: the Rise of Law in Cyberspace, "Stanford Law Review" 1996, vol. 48, no. 5.

Kerikmäe T. (ed.) Regulating eTechnologies in the European Union. Normative Realities and Trends, Cham 2014.

Krasuski A., Status sztucznego agenta. Podstawy zastosowania sztucznej inteligencji, Warsaw 2021.

Kulesza J., Międzynarodowe prawo Internetu, Poznań 2010.

Lai L. and Świerczyński M. (eds.), Prawo Sztucznej Inteligencji, Warsaw 2020.

Leens R., Regulating New Technologies in Times of Change, (in:) L. Reins (ed.), Regulating New Technologies in Uncertain Times, Cham 2019.

Lessig L., Code and Other Laws of Cyberspace, New York 1999.

Lessig L., Code is Law: On Liberty in Cyberspace, "Harvard Magazine", https://harvardmagazine.com/2000/ 01/code-is-law-html.

Liability for Artificial Intelligence and other emerging digital technologies: Report from the Expert Group on Liability and New Technologies – New Technologies Formation, https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608.

M. Hildebrandt, Algorithmic Regulation and the Rule of Law, "Philosophical Transactions of the Royal Society A" 2018, vol. 376, issue 2128, https://royalsocietypublishing.org/doi/10.1098/rsta.2017.0355.

Magnusson Sjöberg C., Legal Automation, AI and Law Revisited, (in:) M. Corrales, M. Fenwick and Haapio H., Legal Tech, Smart Contracts and Blockchain, Singapore 2019.

McCarthy J., Minsky M.L., Rochester N. and Shannon C.E., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf.

Menthe D.C., Jurisdiction in Cyberspace: a Theory of International Spaces, "Michigan Telecommunications and Technology Law Review" 1998, no. 69.

Minsky M., Perceptrons: An Introduction to Computational Geometry, Massachusetts 1969.

Minsky M., The Emotion Machine. Commonsense Thinking, Artificial Intelligence, and the Future of the Human Mind, New York/London/Toronto/Sydney 2007.

Nanda R., Siragusa G., Di Caro L., Boella G., Grossio L., Gerbaudo M. and Costamanga F., Unsupervised and Supervised Text Similarity Systems for Automated Identification of National Implementing Measures of European Directives, "Artificial Intelligence and Law" 2019, vol. 27.

National Artificial Intelligence Strategy of the Czech Republic, https://www.mpo.cz/assets/en/guidepost/for-the-media/press releases/2019/5/NAIS_eng_web.pdf.

Prabucki R., Szostek D. and Wyczik J., Prawo jako kod, (in:) D. Szostek (ed.), Legal tech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym, Warsaw 2021.

Proposal For A Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts Com/2021/206 Final, https://Eur-Lex.Europa.Eu/Legal-Content/EN/TXT/?Uri=CELEX:52021PC0206.

Railas L., The Rise of the Lex Electronica and the International Sale of Goods, Helsinki 2004.

Recommendation of Committee of Ministers No. 2102 (2017) about technological convergence, artificial intelligence and human rights (Doc. 14432).

Recommendation of the Council on Artificial Intelligence, OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

Recommendations on regulation, innovation and finance: Final Report to the European Commission, 01.12.2019, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf.

Report with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), https://www.europarl.europa.eu/doceo/document/A-9–2020-0178_EN.html.

Responsibility and AI: Council of Europe study, 21.12.2019, https://rm.coe.int/ responsability -and-ai-en/168097d9c5.

Schrebak S., Integrating Computer Science into Legal Discipline: The Rise of Legal Programming, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496094.

Szostek D. (ed.), Legal tech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym, Warsaw 2021.

Szostek D., Blockchain and Law, Baden-Baden 2019.

Szostek D., Czynność prawna a środki komunikacji elektronicznej, Krakow 2004.

Szostek D., Sztuczna inteligencja a kody. Czy rozwiązaniem dla uregulowania sztucznej inteligencji jest smart contract i blockchain? (in:) L. Lai and M. Świerczyński (eds.), Prawo Sztucznej Inteligencji, Warsaw 2020.

Szpringer W., Blockchain jako innowacja systemowa. Od Internetu informacji do Internetu wartości, Warsaw 2018.

Świerczyński M. and Lai L., Prawo Sztucznej Inteligencji, Warsaw 2020.

Tegmark M., Życie 3.0. Człowiek w Erze sztucznej Inteligencji, Warsaw 2019.

The European Commission's high-level expert group on artificial intelligence, A definition of AI: Main capabilities and scientific disciplines. Definition developed for the purpose of the deliverables of the High-Level Expert Group on AI, Brussels, 18.12.2018, https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines.

The High-Level Expert Group on Artificial Intelligence European Commission Directorate-General for Communications Networks Technology, 20.09.2018.

Trudel P., La lex electronica, (in:) C.A. Morand (ed.), Le droit saisi par la mondialisation, Brussels 2001.

Turing A., Computing Machinery and Intelligence, "Mind" 1950, vol. 49, no. 236.

Turner J., Robot Rules. Regulating Artificial Intelligence, Cham 2019.

Wendehorst C.H., Safety and Liability Related Aspect of Software, 17.06.2021, https://digital-strategy.ec.europa.eu/en/library/study-safety-and-liability-related-aspects-software.

Werbach K., The Blockchain and the New Architecture of Trust, London 2018.

White Paper On Artificial Intelligence. A European approach to excellence and trust, COM(2020) 65 final, European Commission, https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

Wiebe A., Die elektronische Willenserklarung, Tubingen 2002.

Wood G., Ethereum: A Secure Decentralized Generalized Transaction Ledger (EIP-150 revision), http://gavwood.com/Paper.pdf.

Wright N.D. (ed.), Artificial Intelligence, China, Russia, and the Global Order, Maxwell 2019.

Yao M., Jia M. and Zhou A., Applied Artificial Intelligence. A Handbook for Business Leaders, Middletown 2018.

Zalewski T., Definicja sztucznej inteligencji, (in:) L. Lai and M. Swierczyński (eds.), Prawo Sztucznej Inteligencji, Warsaw 2020.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.04

Received: 12.01.2021
Accepted: 10.04.2021

Patrycja Dąbrowska-Kłosińska
Queen's University Belfast, Northern Ireland
p.dabrowska@qub.ac.uk
ORCID ID: https://orcid.org/0000–0002-3581–3226

Agnieszka Grzelak
Kozminski University in Warsaw, Poland
agrzelak@kozminski.edu.pl
ORCID ID: https://orcid.org/0000–0002-5867–8135

Agnieszka Nimark
Cornell University, United States of America
Barcelona Centre for International Affairs (CIDOB), Spain
an355@cornell.edu

The Use of Covid-19 Digital Applications and Unavoidable Threats to the Protection of Health Data and Privacy[1]

Abstract: This paper starts with a dilemma. How to ensure the adequate protection of individual health data and privacy in a global pandemic, which has intensified the use of digital applications for the purposes of data sharing and contact-tracing? There is no simple answer to this question when choosing between the protection of public health and individual privacy. However, the history of the existing case-law regarding infectious diseases control, both Polish and European, teaches about numerous examples in which health data and privacy were not adequately protected, but, on the contrary, were misused leading to human rights infringements. In light of this case law and public health ethics, this paper argues radically that the use of digital applications to fight the Covid-19 pandemic has not been sufficiently justified at least in the Polish context. Especially, unconvincing benefits from the use of these

1 This research was in part supported by the project THEMIS (2018–2021; Principal Investigator: Patrycja Dąbrowska-Kłosińska) of the EU Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No. 746014, which is hereby acknowledged.

tools do not outweigh the likelihood of human rights infringements with far-reaching consequences for political, social and economic rights now and in the future. In its novelty, this article combines a historical-legal method with the concept of public health ethics and a human rights-based approach and to foster further research and discussion. The text also responds to the pressing need to analyze those human rights issues embedded in the Polish reality.
Keywords: COVID-19, digital applications, European Court of Human Rights, fundamental rights, global health threats, health data protection, privacy, surveillance

Introduction

The Covid-19 pandemic has drawn urgent attention to the known legal and ethical dilemma of how to ensure the adequate protection of individual privacy in times of "mass surveillance" technologies and global health threats of infectious diseases which require data sharing and contact-tracing.[2] Answers to this dilemma and the practical feasibility of ensuring an adequate level of protection in case of sensitive health data, particularly prone to infringements and misuse, have been challenged by the development of modern technologies of big data algorithms and artificial intelligence[3]. These issues have already been highlighted by scholars in surveillance and security, human and constitutional rights and public health law studies[4].

Yet, shortly after the coronavirus outbreak, many governments began employing digital tools, especially individual mobile phone applications (so-called:

2 Report of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, 3.8.2018, https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx (accessed 28.04.2021), pp. 5–8ff. See also for example: N. Ram, D. Gray, Mass surveillance in the age of COVID-19, 'Journal of Law and the Biosciences' 2020, vol. 7, no. 1, p. 1–17 and the sources provided there.

3 S.L. Roberts, Big Data, Algorithmic Governmentality and the Regulation of Pandemic Risk, "European Journal of Risk Regulation" 2019, vol. 10, Issue 1, pp. 94–115; cf. W.K. Mariner, Reconsidering Constitutional Protection for Health Information Privacy, 'Journal of Constitutional Law' 2016, vol. 18, no. 3, pp. 975–1054, in the U.S. context.

4 In the Polish scholarship, see e.g. K. Chałubińska-Jentkiewicz, M. Nowikowska, Bezpieczeństwo, tożsamość, prywatność – aspekty prawne, Warsaw 2020; K. Łakomiec, Konstytucyjna ochrona prywatności. Dane dotyczące zdrowia, Warsaw 2020; K. Świtała, Interoperacyjność i bezpieczeństwo danych medycznych w systemach e-zdrowia i telemedycynie, (in:) I. Lipowicz, M. Świerczyński and G. Szpor (eds.), Telemedycyna i e-Zdrowie. Prawo i informatyka, Warsaw 2019; M. Rojszczak, Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji, Warsaw 2019; P. Dąbrowska-Kłosińska Stosowanie unijnych przepisów o transgranicznych zagrożeniach dla zdrowia, a ochrona danych osobowych w UE, „Przegląd Prawa i Administracji Acta Universitatis Wratislaviensis" 2016, vol. 107, pp. 53–81; A. Grzelak, Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości, Warsaw 2015; W.R. Wiewiórowski, Profilowanie osób na podstawie ogólnodostępnych danych, (in:) A. Mednis (ed.), Prywatność a ekonomia: ochrona danych osobowych w obrocie gospodarczym, Warsaw 2013.

"Apps"), to fight the pandemic by controlling the way people move, collecting information about infected people and people with whom the infected had contact, and serving as communication tools. Consequently, a pressing need has emerged to re-examine the use of these applications for public health protection in the context of individual privacy. Specifically, crucial questions concern the purposes which these digital applications or systems really serve and their effectiveness; their possible violation of individual privacy in the public dimension while protecting the collective right to health; the justification of limiting the right to privacy especially in light of the proportionality analysis; and, finally, the implications for other human rights.

The development and use of digital tools caused the world-wide reaction of various actors and stakeholders. To begin with, the response by policy authorities and civil society shall be mentioned. A considerable number of documents was issued by the international organizations concerned with the use of these tools, data transfers and human rights protection in the context of fighting the pandemic: EU institutions[5], the Council of Europe[6] and the OECD[7]. Both civil society and private actors also published reports to emphasize the complexity of the issue[8].

5 See e.g. European Commission, Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, 2020/C 124 I/01, C/2020/2523 (O.J. C 124I, 17.4.2020), pp. 1–9; European Data Protection Supervisor (EDPS), EU Digital Solidarity: a call for a pan-European approach against the pandemic, 6.4.2020, https://edps.europa.eu/sites/edp/files/publication/2020–04-06_eu_digital_solidarity_covid19_en.pdf (accessed 28.4.2021); Joined statement on the right to data protection in the context of the COVID-19 pandemic by A. Pierucci and J.-P. Walter, 30.3.2020 https://rm.coe.int/covid19-joint-statement/16809e09f4 (accessed 28.4.2021); European Data Protection Board (EDPB), Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21.4.2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf (accessed 28.4.2021); Fundamental Rights Agency (later: FRA), Coronavirus Pandemic in the EU – fundamental rights implications: with a focus on contact-tracing apps, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf (accessed 28.4.2021).

6 Protection of health-related data – Recommendation CM/Rec(2019)2 adopted by the Committee of Ministers of the Council of Europe, 27.3.2019.

7 OECD Policy Responses to Coronavirus (COVID-19), Ensuring data privacy as we battle COVID-19, 14.4.2020 http://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19–36c2f31e/#section-d1e690 (accessed 28.4.2021).

8 Privacy leaders, https://iapp.org/resources/article/privacy-leaders-views-impact-of-covid19-on-privacy-priorities-practices-programs/ (accessed 28.4.2021); Deloitte Report, Privacy and Data Protection in the age of COVID-19, https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-risk_privacy-and-data-protection-in-the-age-of-covid-19.pdf (accessed 28.4.2021).

Next, the state of the art in the scholarship needs to be outlined. The *problematique* has been extensively explored by the academia[9]. The debate has been inter-disciplinary and thematically and territorially wide-ranging. The ethical analyses have mushroomed, including those which offer guidelines to be respected by policy-makers[10]. The legal studies examine the protection of health data privacy in times of Covid-19 contact-tracing generally[11] and digital applications specifically[12], and they warn of threats from authoritarian regimes not aligning to the rule of law[13]. Several common threads can be identified in these analyses, namely: (i) they investigate whether and how the protection of ethical principles and human rights can be ensured when using digital tools/applications to fight the pandemic; (ii) they scrutinize the existing guarantees of the right to privacy and data protection provided by the present European legal system and/or the scope of lawful limitations of those rights; and (iii) they generally accept that the protection of public health may justify the use of digital tools. Further, to understand the limitations of the right to data protection, this scholarship usually refers to the digital environment case law and/or to security threats-related case law[14], neither of which is directly health-related, which may imply different protection standards. In other words, while fearing possible infringements, the majority of legal studies focus on *de lege lata* and *de lege ferenda* arguments using the method of deduction to infer opinions about the present (the Covid-19 applications and the relevant

9 M. Kędzior, The right to data protection and the COVID-19 pandemic: the European approach, „ERA Forum" 2021, no. 21, pp. 533–543; W.R. Wiewiórowski, Rola Unii Europejskiej w koordynacji zastosowania narzędzi informatycznych do walki z pandemią, „Europejski Przegląd Sądowy" 2020, no. 6, pp. 20–33.

10 C. Pagliari, The ethics and value of contact tracing apps: International insights and implications for Scotland's COVID-19 response, "Journal of Global Health" 2020, vol. 10; F. Lucivero, N. Hallowell, S. Johnson , B. Prainsack, G. Samuel and T. Sharon, COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale, "Journal of Bioethical Inquiry" 2020, no. 17, pp. 835–839.

11 H. van Kolfschooten, A. de Ruijter, COVID-19 and privacy in the European Union: A legal perspective on contact tracing, "Contemporary Security Policy" 2020, vol. 41, Issue 3, pp. 478–491.

12 See A. Michałowicz, Stosowanie aplikacji mobilnych podczas pandemii COVID-19 z perspektywy ochrony danych osobowych, "Europejski Przegląd Sądowy" 2020, no. 6, pp. 34–42; L. Bradford, M. Aboy and K. Liddell K., COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes, "Journal of Law and the Biosciences" 2020, vol. 7, no. 1, pp. 1–33; P.H. O'Neill, T. Ryan-Mosley and B. Johnson, A flood of coronavirus apps are tracking us. Now it's time to keep track of them, "MIT Technology Review", 7 May 2020, https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker (accessed 28.4.2021).

13 M. Rojszczak Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa autorytarnego, „Acta Universitatis Wratislaviensis - Studia nad Autorytaryzmem i Totalitaryzmem" 2020, vol. 42, no. 2, pp. 207–243.

14 *Ibidem*; H. van Kolfschooten, A. de Ruijter, COVID-19, *op.cit.*

legal and practical framework) and make recommendations for the future (about their potential safe use).

We appreciate the importance of the above-mentioned studies. However, this article takes a different point of departure. In its novelty, it combines a historical-legal method with the concept of public health ethics and a human rights-based approach to argue that digital applications likely cause human rights infringements and that legal guarantees are often disregarded.

First, methodologically, we refer to the past to understand the present and offer some lessons for the future. We thus employ the historical-legal method to trace past violations and unconstitutionalities in the context of health data protection case-law where infectious diseases were at issue. We use the examples of judicial decisions that established protection standards to show that unconvincing benefits from the use of digital applications for public health protection do not outweigh the likelihood of rights violations with far reaching consequences. By doing so, we follow the approaches that advocate the inquiries about the past in legal analyses of the health and human rights field[15]. The human and constitutional rights framework applicable in Poland offers the normative orientation for the text (the Polish Constitution, the EU Charter for Fundamental Rights "CFR", and the European Convention for Human Rights "ECHR").

Second, we take the concepts of George Annas and Wendy Mariner on the need for application of public health ethics to control government actions in health. They admit that it is hard "to define a set of ethical principles unique to public health", and they claim to link human and constitutional rights, health law and (medical) ethics to implement values such as equality, justice and non-discrimination[16]. They emphasize that "public health is a social endeavor"[17] and thus must be assessed within social and democratic institutions where governments are obliged to respect, protect and fulfil human rights, which means adhering to the rule of law more generally. They highlight that the *methods* of reaching public health goals as such can be ethically controversial (and not the aim as such) and claim that governments should show (burden of proof) that their public health policy is justifiable and necessary.

Third, we accept that the right to health data protection may need to be lawfully limited to implement contact-tracing procedures and infectious diseases control measures to fight the pandemic. However, we question the justification of limitations,

15 G.J. Annas, Worst Case Bioethics, Oxford/New York 2011; T. Murphy, Health and Human Rights' Past: Patinating Law's Contribution, "Health and Human Rights Journal" 21 November 2019. Cf. also P. Alston, Does the past matter? On the origins of human rights, "Harvard Law Review" 2013, vol. 126, no. 7, pp. 2043–2081.

16 See G.J. Annas and W. K. Mariner, (Public) Health and Human Rights in Practice, "Journal of Health Politics, Policy and Law" 2016, vol. 41, no. 1, pp. 129–133 for the explanation of the possible conceptualisation of public health ethics.

17 *Ibidem*, p. 130.

including their proportionality in case of digital tools, while looking at the seriousness of possible immediate consequences for human rights, including political, social and economic rights, and the rule of law. We also argue that the value of protecting health privacy should be prioritized in pandemics, because the chronic emergency situations may encourage loosening the basic principles of data protection, which in turn may lead to the abuse of these data.

Finally, the above method, frames and approach allow us to argue *radically* that there has not been sufficient justification for the use of individual mobile phones digital applications for contact-tracing and quarantine control to fight the Covid-19 pandemic, at least, currently, in Poland. To present the argument, the text proceeds as follows: section 2 describes the digital applications used in Poland during the Covid-19 pandemic; section 3 presents the past case-law regarding the health data protection and privacy, its limitations and infringements; and section 4 contains an appraisal in light of public health ethics. The last section offers conclusions.

1. The Polish Covid-19 Applications and Privacy Threats in Comparative Perspective

A wide variety of applications have been in use during the Covid-19 pandemic, which can be divided broadly in three types: 1) contact–tracing applications that make users aware of the interaction with the virus; 2) self-assessment applications that inform users about Covid-19 risks, symptoms and steps to follow when they emerge; and 3) quarantine-enforcement applications that report on quarantined people. The following sections present analytically the applications used in Poland to combat Covid-19 against the comparative background of other European states to highlight doubts around their design, mode of use and legal framework constituting threats to privacy rights[18].

1.1. The contact-tracing application: ProteGO Safe

From a public health perspective, the contact-tracing applications seem most promising to help governments manage the spread of diseases and complement traditional, in-person, contact-tracing. They are designed to inform users of their contact with a person who tested positive for Covid-19 and to upload data on the phone, after which the system sends a notification to phones of those who have been

18 See also: Theme 3: Covid-19, privacy rights and cyber security risks, "Covid-19 Resources", Pinciples for Responsible Investment, 7.9.2020, https://www.unpri.org/covid-19-resources/theme-3-covid-19-privacy-rights-and-cyber-security-risks/6343.article (accessed 28.4.2021).

in close contact with the person[19]. The applications rely on various technologies to track and store users' locations: either Bluetooth- (proximity data) or network- and/or GPS-based[20]. Bluetooth-based contact-tracing applications are more common; individuals download an application that detects other smartphones' Bluetooth signals. These applications follow "a decentralized model" (with users' data produced and stored locally on their devices), which better protects personal data as compared to "centralized models" (where users' data are stored and processed on some central servers).

"Trace Together" was one of the first contact-tracing applications introduced in the world (Singapore)[21]. In the EU, the applications were either available (Austria, Bulgaria, Cyprus, Czech Republic, Lithuania, Spain, and Poland) or under development by the end of April 2020 in most states (including Belgium, Germany or Denmark)[22]. As analyzed by the Fundamental Rights Agency ("FRA"), the majority of these applications were Bluetooth-based and relied on "a decentralized approach" following the recommendations of the European Commission and the European Data Protection Board[23].

The Polish Ministry of Digital Affairs designed an application called STOP COVID –ProteGO Safe[24]. It was developed to track the location and health data of users, disseminate personalized guidance in case of contact with an infected person, transmit relevant information directly to the Chief Sanitary Inspector (data controller) and provide users with verified medical advice. The risk-assessment was supplemented with a self-diagnostic monitoring tool and a dedicated helpline[25]. The ProteGO thus combined contact-tracing and self-assessment (see below). The application used Bluetooth-based technology to record data on the proximity to other users with the application installed on their devices. As the use of the application was

19 For technical details see: E. Kusat Kaya, Safety and privacy in the time of covid-19: contact tracing applications, Centre of Economics and Foreign Policy Studies, https://www.jstor.org/stable/resrep26089?seq=1#metadata_info_tab_contents (accessed 28.4.2021).

20 Cf. Norwegian Infection Stop, 20 April 2020, Privacy International, https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps (accessed 28.4.2021).

21 In line with: eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19, Common EU Toolbox for Member States, 15.4.2020, p. 9, https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf (accessed 28.4.2021).

22 FRA, Coronavirus pandemic, *op. cit.*, pp. 52–53.

23 EDPB, Guidelines 04/2020, *op. cit.*

24 Personal data is processed on the basis of Art. 6, Sec. 1, letters c) and e) GDPR in connection with the performance of a task in the public interest, resulting from Art. 1, 2, 3, 6 and 81, Sec. 1, 4 and 5 of the Act of 14 March 1985 on the State Sanitary Inspection (consolidated text Journal of Laws 2019, item 59). See Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (O.J. L 119, 4.5.2016), p. 1 ("GDPR").

25 eHealth Network, Mobile, *op. cit.,* p. 10.

voluntary, only 1.9% of the Polish population downloaded the application between June-September 2020. That was one of the lowest take-up levels in Europe, which affected the effectiveness of the costly system[26]. ProteGO Safe was also criticized for flaws in privacy protection and functionality[27].

Following the claims that the system was not effective, the Ministry held a consultation with the number of the Polish non-governmental organizations (NGOs), appointed a ProteGO Safe expert team, and finally prepared and published a set of documents: a privacy policy, a risk analysis for personal data protection, a FAQ document and a security audit report. As a result, the NGOs' evaluation of the application was positive, in principle, regarding data protection safety and compliance with the principles of applications' good design[28]. The application neither monitors the location nor collects any redundant data; it ensures encryption of transmitted messages (keys) and anonymity, and it guarantees data security.

Notwithstanding these measures, the doubt about the possibility of health data misuse remains regarding the practical use of the application. We will return to the analysis of the measures in section 4 below.

1.2. Self-assessment applications

The second type of developed applications serves information providing and gathering purposes. People wishing to know more about Covid-19, possible treatment and their health can assess either prognoses about the likelihood of infection or information about the outbreak. They allow users voluntarily to upload their anonymized data and symptoms to help governments to map the spread of the disease. While these applications typically neither ask for individual, identifiable data nor transfer them to third parties, some of the applications still do.

These tools preceded the pandemic and were offered by private companies before[29]. However, during the pandemic, state governments became involved in using them. The health reporting applications and websites exist in many EU states[30]; likewise, the World Health Organization has been involved in developing an

26 B. Koschalka, Uptake of Covid contact tracing app under 2% in Poland, among the lowest rates in Europe, 11.9.2020, Notes from Poland, https://notesfrompoland.com/2020/09/11/uptake-of-covid-contact-tracing-app-under-2-in-poland-among-the-lowest-rates-in-europe/ (accessed 28.4.2021).

27 See: Coronavirus contact tracing reignites Polish privacy debate, 'Deutsche Welle', https://www.dw.com/en/coronavirus-contact-tracing-reignites-polish-privacy-debate/a-53600913 (accessed 28.4.2021).

28 A. Obem, ProteGO Safe: instalować czy nie?, 3.8.2020, https://panoptykon.org/czy-instalowac-protego-safe and links on this webpage (accessed 28.4.2021).

29 See for example in Canada: https://preworkscreen.com/ (accessed 28.4.2021).

30 Coronavirus Pandemic In The EU – Fundamental Rights Implications: With A Focus On Contact-Tracing Apps, 21 March – 30 April 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf, p. 53 (accessed 28.4.2021).

application that provides medically-approved information and advice to users based on their symptoms[31]. In some countries, the contact-tracing and self-assessment applications are developed together as a one integrated system (e.g., the ProteGO Safe).

1.3. The Kwarantanna domowa application

The third type of Covid-19 applications is comprised of tools that track people in quarantine to control their compliance with isolation orders. These applications are required to be used by visitors and travelers in some states[32], while in others[33], they have been used by public authorities to communicate Covid-19 information and quarantine guidelines and to prevent violations of self-quarantine orders.

Similarly, in Poland, the application Kwarantanna domowa (in English: "home quarantine") was introduced for the individuals subjected to mandatory house quarantine, after possible Covid-19 exposure, to control whether they respected the quarantine orders[34]. The application uses geo-location and face recognition technology and obliges concerned individuals to upload their location and photo for identity verification upon request by the police. The application collects the following data: citizen ID – technical identifier of the citizen, first name, surname, phone number, declared residence address, photo, location of the citizen and the end date of quarantine. Compliance is mandatory unless one declares: (i) non-subscription/non-use of the telecommunications network; (ii) non-possession of an adequate mobile device to install the software; or (iii) a visual impairment (blind or partially sighted)[35].

The Kwarantanna domowa raised concerns about the possible violation of users' rights to personal data protection. These concerns were raised by both public institutions and academia. First, the Polish Commissioner for Human Rights ("the Polish CHR") asked the President of the Office for Personal Data Protection and the Prime Minister for an opinion on the matter[36]. These governmental authorities

31 See: COVID-19 App, https://worldhealthorganization.github.io/app/ (accessed 28.4.2021).

32 E.g. Russia and Hong Kong, see: There's an app for that: Coronavirus apps, 20.4.2020, https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps (accessed 28.4.2021).

33 Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics, 23.4.2020, https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/ (accessed 23.4.2020) (The South Korean Self-quarantine Safety App).

34 J. Van Zeben and B.A. Kamphorst, Tracking and Nudging through Smartphone Apps: Public Health and Decisional Privacy in a European Health Union, "European Journal of Risk Regulation" 2020, vol. 11, Issue 4, p. 838.

35 Art. 7e of the Act of 2 March 2020 on special solutions related to the prevention, counteraction and combating of COVID-19, other infectious diseases and the crisis situations caused by them (consolidated text Journal of Laws 2020, item 1842).

36 Aplikacja „Kwarantanna domowa" budzi wątpliwości obywateli. Rzecznik pisze do premiera, 13.11.2020, https://www.rpo.gov.pl/pl/content/rpo-do-premiera-aplikacja-kwarantanna-domowa-

obviously declared that appropriate encryption methods had been used and that the data processing model complied with the requirements set out in the General Data Protection Regulation ("GDPR")[37]. Second, two specific allegations against the application's solutions from the perspective of data protection were enumerated in the scholarship[38]: (i) for unknown reasons, the data stored on centralized servers will be kept for 6 years, except for theoretically deleted images when the user deactivates the account, if a user does so; (ii) for unknown purposes, the number of actors granted access by law to the data processed in the application and the system is unjustifiably large, including the Police Forces Headquarters, the Provincial Police Headquarters, the voivodes (the governmental organs of regional administration), e-Health Center, the National Research Institute, as well as the third parties: companies Take Task S.A. and Tide Software Sp. z o.o. (entities that support the technical side of the application).

Before proceeding to a further assessment, the objective of the next section is to show the breadth of possible implications for individual human and constitutional rights of the health data access by public and private actors, including for legitimate purposes, and to claim that the sensitivity of the data and often the fear of disease both create an additional temptation for the misuse.

2. The Infringements of the Right to Health Data Protection and Privacy: Lessons from the European and Polish Case-law Histories

To begin with, several matters merit explanation.

First, we follow the approach of the courts, both the Polish Constitutional Tribunal (pre-2015, "CT") and the EU Court of Justice ("CJEU") and refer to both rights together: the right to respect for private (and family) life and the right to the protection of personal data[39]. Both rights are closely related, protect similar values (the autonomy and human dignity of individuals) and are quintessential for the exercise of other fundamental freedoms. Second, we treat the normative framework applicable to the protection of individual rights, within which the relevant case-law has developed, as a joint matrix of the Polish (the Constitution and laws) and European provisions (CFR and ECHR) with the GDPR (a directly applicable EU secondary law) as a key reference for data protection in the EU. Third, the subsequent

budzi-watpliwosci (accessed 28.4.2021).

37 MC zapewnia: aplikacja mobilna „Kwarantanna Domowa" zgodna z wymogami RODO, 30.11.2020, https://www.rpo.gov.pl/pl/content/mc-zapewnia-rpo-aplikacja-kwarantanna-domowa-zgodna-z-rodo (accessed 28.4.2021).

38 A. Michałowicz, Stosowanie, *op. cit.*, pp. 34–42.

39 Judgment of the Constitutional Tribunal of 18 December 2014, K 33/13, OTK-A 2014, no. 11, item 120, point 4.4; Judgment of the CJEU of 9 November 2010 on joined cases of Volker and Markus Schecke GbR and Hartmut Eifert v Land Hessen, C-92/09 and C-93/09, point 52.

sections depict the lessons from known infringements of the right to health privacy through the lens of case-law histories in judicial proceedings in both Polish and European courts. The text does not aspire to present a systematic history of the jurisprudence on judicial standards for personal health data protection. The cases were purposefully selected to show health data misuse in various contexts important for persons' lives: work environment, judicial proceedings, media and international mobility. Specifically, we wish to show how particularly damaging health data misuse can be for individuals concerned and their human rights in the social and economic context *notwithstanding* the extensive legal guarantees to ensure the protection of individual health data privacy and its value. This connects to the initial ethical dilemma of this text and the known history of human rights violations in the name of public interests, including public health (understood broadly). Lastly, the first part of the section explains the normative framework for the lawful limitation of health privacy rights.

2.1. The right to health data protection and privacy and their limitations

The following norms apply to possible limitations of the right to health privacy.

The Polish Constitution protects both the right to health privacy (Art. 47) and the right to the protection of health data (Art. 51)[40]. These rights can be lawfully limited in accordance with Art. 31(3) of the Constitution, which requires compliance with basic conditions of legality and proportionality *sensu largo*. That is, the restriction must be: (i) based on law; (ii) necessary in a democratic state for one of the enumerated purposes; and (iii) respectful of the core of rights, i.e., proportionality *sensu stricto*[41]. The public health is among the legitimate reasons for limitation, and it corresponds to the state obligation to prevent and combat epidemic diseases provided by Article 68 of the Constitution[42].

Further, the Constitution does not define "health data" explicitly[43], but a broad definition is included in the GDPR (Art. 4, point 15), which also states that personal "data concerning health" belong to the category of sensitive data the processing of which is prohibited generally unless specific exceptions apply (Art. 9(1) "special

40 Judgment of the Constitutional Court in the already mentioned case K 33/13 and of 19 February 2002 in case U 3/01.

41 P. Tuleja, Komentarz do art. 31 Konstytucji RP, (in:) P. Tuleja (ed.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warsaw 2020, p. 114–119; L. Garlicki and M. Zubik (eds.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, Tom I, Warsaw 2016; M. Safjan and L. Bosek (eds.), Konstytucja RP. Tom I. Komentarz do art. 1–86, Warsaw 2016.

42 T. Sroka, Ograniczenia praw i wolności konstytucyjnych oraz praw pacjenta w związku z wystąpieniem zagrożenia epidemicznego, 'Palestra' 2020, no. 6, pp. 75–98 and sources cited therein.

43 M. Florczak-Wątor, Komentarz do art. 51 Konstytucji, (in:) P. Tuleja (ed.), Konstytucja, *op. cit.*, pp. 178–179. See also generally M. Safjan and L. Bosek (eds.), Instytucje Prawa Medycznego. System Prawa Medycznego. Tom 1, Warsaw 2017.

category of data" and Article 9(2)(a-j) "exceptions")[44]. The relevant exceptions may, for example, concern an explicit consent of a person (a); or processing required for "establishment, exercise or defense of legal claims" (f); "for reasons of substantial public interest" (g); "the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee (…)" provided it is undertaken by professionals obliged to professional secrecy (h); "for reasons of public interest in the area of public health", for example, protecting against serious cross-border threats to health (i); and scientific and historical research and statistical purposes (j)[45]. Further conditions, including limitations, with regard to the processing of health data can be introduced by national law.

Certainly, the GDPR enumerated exceptions to health privacy need to be situated and interpreted against the national law systems. In Poland, for example, health data confidentiality is further regulated and protected through various acts. Accordingly, it can also be limited, for example, pursuant to the applicable health laws (in case of patients)[46] or civil and criminal judicial procedures' laws (in case of participants in proceedings)[47].

Further, we can relate the GDPR general prohibition of sensitive data processing to Article 51(2) of the Constitution, which establishes a prohibition of the Polish citizens' data processing by public authorities unless necessary in a democratic society. This requirement functions similarly to the proportionality principle, which brings us back to the point that the constitutionality/lawfulness of a health privacy limitation on the basis of any given exception will still need to meet the conditions of Article 31(3) of the Constitution (see above)[48], and, if the matter falls within the scope of the EU law, the CFR.

---

44 FRA and Council for Europe, Handbook on European Data Protection Law, Luxembourg 2018, pp. 42–45; and P. Dąbrowska-Kłosińska, Tracing Individuals under the EU Regime on Serious, Cross-border Health Threats: An Appraisal of the System of Personal Data Protection, "European Journal of Risk Regulation" 2017, vol. 8, no. 4, pp. 707–710.

45 E.g., Commission Implementing Decision amending Implementing Decision (EU) 2017/253 as regards alerts triggered by serious cross-border threats to health and for the contact tracing of passengers identified through Passenger Locator Forms, 25.03.2021, no ref. yet.

46 E.g., M. Wałachowska, Ochrona danych osobowych w prawie cywilnym i medycznym, Toruń 2008; M. Jackowski, Ochrona danych medycznych, Warsaw 2011.

47 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (O.J. L 119, 4.5.2016). See also A. Grzelak (ed.), Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Warsaw 2019.

48 M. Florczak-Wątor, Komentarz, *op.cit.*, p. 179.

Accordingly, Articles 7 and 8 of the CFR constitute right to privacy and data protection respectively in the EU, and a lawful limitation of the rights needs to respect Article 52(1) CFR, including in the context of public health[49]. Consequently, every transfer of health information by a public authority may be justified only if: (i) it is "in accordance with the law"; (ii) it pursues an objective which is exhaustively listed; and (iii) it is "strictly necessary" and proportional to achieve that objective[50]. In addition, since the CJEU makes direct references to the European Court of Human Rights' ("ECtHR") privacy case-law while considering data protection issues, the limitations which may lawfully be imposed on the right to protection of health privacy in the EU correspond to those accepted under Article 8 ECHR (the right to respect for private and family life)[51], which also stems from Article 52(3) CFR[52].

To put it simply, every judicial review of a possible rights' violation will need to establish: (i) the occurrence of interference with health privacy either with or without justification (i.e., adequate legal basis, legitimate aim/exception); and (ii) the necessity and proportionality of the applicable exception to health data processing prohibition (e.g., public health surveillance, serious health threat, etc.). In the context of a given claim in question, the scope and content of judicial review will depend on a court considering which specific legal framework will be applied as a source of human rights protection (that is, whether it shall be a constitutional or ECtHR standard). The court will also decide on a primary point of departure for the interpretation and construction of the standard of review for its ruling, including, e.g., a proportionality assessment.

Let us now turn to the relevant judicial practice.

---

49 Cf. also Judgment of CJEU of 8 April 2014 on joined cases of Digital Rights Ireland and Seitlinger and Others, C-293/12 and C-594/12, point 238.

50 Cf. Judgment of CJEU of 20 May 2003 on joined cases of *Österreichischer* Rundfunk, C-465/00, C-138/01 and C-139/01, points 73–75. See also Judgment of CJEU of 16 December 2008 on the case of Huber v. Germany, C-524/06, point 68.

51 See also Judgment of ECtHR of 29 April 2014 on the case of L.H. v. Latvia, application no. 52019/07; Judgment of ECtHR of 16 February 2000 on the case of Amann v. Switzerland, application no. 27798/95; Judgment of ECtHR of 4 May 2000 on the case of Rotaru v. Romania, application no. 28341/95.

52 Judgment of CJEU of 9 October 2009 on joined cases of Volker and Markus Schecke, C-92/09 and C-93/09, points 51–52, 57, 89. See also P. De Hert and S. Gutwirth, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, (in:) S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), Reinventing Data Protection?, Dordrecht 2009, p. 3.

2.2. Lesson 1: The health data disclosure without consent and freedom of expression

The opening example comes from the ECtHR and concerns press publication of personal health data without consent and its questionable justification through the protection of the freedom of expression and public interest[53].

In January 2001, Lithuania's biggest daily newspaper published a front-page article about the exposure of residents in villages of remote Lithuania to fear of death and the AIDS threat[54]. The text provided the name, private life extensive details and the health status (seropositive and tuberculosis) of Ms. Biriuk. The accuracy of the information was confirmed by the medical staff of a local hospital. National courts found the breach of her privacy, but the damages awarded were derisory. Moreover, the Lithuanian Supreme Court indicated that the personal safety of people living in proximity to those sick with AIDS and dangers from persons whose behavior does not always meet moral standards need to be taken into account as valid arguments[55].

The ECtHR did not agree that "the purported concerns of the local population for their safety were legitimate, either socially or scientifically" and did not justify a publication about the applicant's state of health and her life style. It established a violation of Article 8 ECHR and raised damages awarded to the applicant. Further, the ECtHR emphasized the fact that medical staff's confirmation of the published health data particularly undermined societal trust in the medical profession, and observed that lack of patient confidentiality, especially in case of infectious diseases, affects negatively the willingness of people to HIV-test voluntarily and seek appropriate treatment. The disclosures of health data endanger both individuals concerned and the society at large. The ECtHR also indicated that the state obligation to safeguard medical privacy must be effective and that the allegations about someone's health and personal life cannot be justified by a legitimate public interest and facts-reporting necessary for a debate in a democratic society (Article 10 freedom of expression). The Court explained that disclosure of health data may dramatically affect an individual's private and family life, as well as the individual's social and employment situation[56].

This case is illustrative for several reasons. The societal fear of disease pressures public authorities, including the judiciary, to accept the publication of health data of potentially "dangerous individuals", especially in cases of infectious diseases for the sake of the alleged protection of "public safety interest". As a result, those authorities often follow a paternalistic path, and their behavior leads to stigmatization and

53 Judgment of CJEU of 6 November 2003 on the case of Bodil Lindqvist, C-101/01.

54 Judgment of ECtHR of 25 November 2008 on the case of Biriuk v. Lithuania, application no. 23373/03 and Judgment of ECtHR of 25 November 2008 on the case of Armonienė v. Lithuania, application no. 36919/02.

55 ECtHR case *Biriuk v. Lithuania*, *op. cit*., points 1–10.

56 *Ibidem*, points 34–47.

shaming of individuals, which adversely affects their social lives considerably. Further, it prompts them and others similarly situated to hide their health condition and functions counter-productively to public health protection. Media broadcasters are tempted to publish such information to scandalize and increase sales or to manipulate public opinion and instigate fears. Finally, the ruling also highlights the centrality of consent in health data processing.

The next sections analyze the relevant aspects in the EU and Polish case-law concerning employment relations. These cases demonstrate the breadth of human rights' implications for individuals when their health data are transferred and/or misused in the area of occupational medicine, the right to work and the right to access public service.

2.3. Lesson 2: The misuse of health data, occupational medicine and the right to work

Mr. X took part in a recruitment procedure at the European Commission[57]. During the process, a specific blood test was carried out by a medical officer to establish indirectly his immune deficiency (AIDS), because he had explicitly refused to undergo HIV-antibodies testing. The test was thus carried out and communicated to Mr. X's general practitioner without his consent. As a result, Mr. X was denied employment due to "physical unfitness".

While referring to Article 8 ECHR, the CJEU stated that the right to personal privacy includes keeping secret the state of one's health. It also held that the legitimate interest of institutions in verifying the fitness of future employees (general public interest) can be justified as such, but medical tests cannot be performed against the person's will. It precludes any test which could establish the existence of an illness concerned. An unconsented medical test infringes the very substance of the protected right and constitutes disproportionate and intolerable interference.[58]

The second important case for consideration is that of Ms. F and concerned the transfer, without her consent and knowledge, of her medical file (containing personal health data) between EU institutions for the purposes of a recruitment process[59]. The CJEU referred to Article 8 ECHR again to scrutinize the lawfulness of the interference based on the legitimate aim of pre-recruitment medical examination and emphasized that exceptions must be constructed narrowly out of respect for the principle of

57 Judgment of the Court of 5 October 1994 on the case of X v Commission of the European Communities, C-404/92 P.

58 *Ibidem,* points 1–8, 17–25.

59 Judgment of the Civil Service Tribunal of the 5 July 2011 on the case of V v. European Parliament, F-46/09, points 112–113.

proportionality. The CJEU also cited the ECtHR's restricted margin of appreciation applicable to "extremely intimate and sensitive nature of medical data"[60].

While establishing the violation of the right, the CJEU stated that the right to privacy governs not only a patient's privacy (relating to medical ethics), but also the confidence (trust) in the medical profession and in the health services in general. It underlined that the sole institutional interest does not justify transfer of health data without consent, especially of those stored for another purpose (different recruitment); and that the secret practice of inter-institutional transfer of health data was not acceptable[61].

Finally in a national, Polish case, an inappropriate medical certificate and misconduct by the administrative personnel (who communicated the health data to the company chief) allowed the employer to learn about Mr. P.S.'s seropositive status. It resulted in his immediate dismissal without any grounds. The claim concerned damages, and, in 2019, the Polish Regional Court adjudicated high compensation based on discrimination in employment of the person concerned[62].

The cases show vividly the co-relation between the infringement upon privacy rights, the right to work and discrimination in access to employment by public and private actors. Discriminatory recruitment and redundancies resulting from disease stigma often occur because of unlawful health data transfer, fear among co-employees, but also lack of medical knowledge and ignorance of the actual health condition of persons concerned[63]. The philosophy of automatic dismissal of those affected by a disease is unfortunately not limited to discriminatory treatment, but can also be provided by law. The next section depicts this issue.

2.4. Lesson 3: The use of health data and access to public service and employment

The Polish CT's judgment (2009) concerned the provisions that regulated the fitness of the candidates to the Polish police forces and the respective powers of medical committees[64]. The applicable law mandated an automatic classification of seropositive persons serving in the police to the category of persons "entirely

60 *Ibidem,* points 122–3, 131, referring to judgment of ECtHR of 25 February 1997 on the case of Z v Finland, application no. 22009/03.

61 Judgment of the Civil Service Tribunal of the 5 July 2011 on the case of V v. European Parliament, F-46/09, points 128–140.

62 Judgment of the District Court in Warsaw of 14 May 2019, XXI Pa 106/19, http://www.ptpa.org.pl/site/assets/files/1855/sygn__akt__xxi_pa_106_19.pdf (accessed 29.04.2021).

63 Judgment of the Supreme Court of 2 October 2012, II PK 82/12, OSNP 2013, no. 17–18, item 202; Judgment of ECtHR of 3 October 2013 on the case of I.B. v. Greece, application no. 552/10; Judgment of the EU Court of First Instance of 9 June 1994 on the case of X v. Commission, T-94/92.

64 Judgment of the Constitutional Tribunal of 23 November 2009, P 61/08, OTK 2009, no. 10A, item 150.

incapable of service" and automatic dismissal from work. There was no exception to this rule and no possibility of its disapplication.

After an exemplary analysis of the proportionality of the restriction of the right to access public service (Articles 60 and 31(3) of the Constitution), the CT found that the objectives of ensuring the good health of police personnel and the public health protection from disease, which realize the state duty to combat epidemics under Article 68(4) of the Constitution, do not justify the automatism and restrictiveness of the legislative solution considered. The CT indicated that the law should aim to protect both public health *and* the right to access public service. It stated that the contested regulation infringed upon human dignity and led to a "mechanical" exclusion of HIV-infected persons despite the psychophysical conditions (service suitability), a state of health of an asymptomatic person, and circumstance of infection, which may be caused by the service itself, undertaken in the social interest. The CT also recognized that the relation between the HIV-status and the right to work/public service is an important social problem (disease stigma) and that the disproportionality of contested rules could be counterproductive and, in fact, lead to hiding infections and increased health threats. It supported its arguments by referring to the EU and US case-law and to the UN guidance on HIV and human rights, which recommend that no mandatory testing be conducted in recruitment processes, that the stability of employment be guaranteed as long as a person is able to work, and that the protection ensure against discrimination and stigmatization in the workplace.

The next case of Mr. P.T. concerns disclosure of his HIV-status in a certificate exempting him from military service, the presentation of which was obligatory upon renewing the identity documents and in job applications. The ECtHR held that there had been a violation of Article 8 ECHR, finding that the disclosure of seropositive status in the certificate concerned had breached the privacy rights. It noted that the Moldovan Government had not specified which "legitimate aim" of limitation of Article 8 ECHR had been pursued by revealing the illness and including sensitive information about the applicant in the certificate, which could be requested in a variety of situations, and where the medical condition was of no relevance. The ECHR found that such a serious interference with the right was disproportionate[65].

The judgments show that inadequately and disproportionately implemented public health protection from contagious diseases can easily lead to unnecessary breaches of health confidentiality, the exclusion based on normative framework, and ultimately, discrimination based on health. Moreover, the fear of diseases and the temptation to exploit health data as a discriminating tool of exclusion and oppression appear also instructively in the histories of judicial proceedings where medical data

65 Judgment of ECtHR of 26 May 2020 on the case of P.T. v. the Republic of Moldova, application no. 1122/12. See also judgment of the Constitutional Tribunal of 19 June 2018, SK 19/17, OTK-A 2018, item 42.

were unnecessary disclosed during court trials with no connection to legal actions. Three cases illustrate the relevant matters.

2.5. Lesson 4: The disclosure of health data in judicial proceedings

In 1999, Mr. Panteleyenko faced criminal charges for alleged abuse of power and forgery of documents[66]. His office was searched as part of the investigation. During one of the proceedings, Mr. Panteleyenko denied having had mental health issues and produced a certificate from a psychiatric hospital supporting this assertion. The certificate was challenged, and the court requested his health records. As a result, his health record (explaining his treatment of mental illness) was provided by the hospital and read aloud at a public hearing.

The ECtHR found the violation of the applicant's right to privacy (Article 8 ECHR) due to the search of his office and the disclosure of his confidential health data in court, which was beyond what was necessary for the proceedings, as the information was not "important for an inquiry, pre-trial investigation or trial". The ECtHR explained that both the storing and use of information about an individual's private life by a public authority constitutes an interference with Article 8. Moreover, the ECtHR noted that the details at issue were irrelevant for the outcome of the litigation (i.e., establishing whether the alleged statement was made and assessing whether it was libelous) and that the domestic court's request for health information was redundant and unlawful according to the national law. This case highlights the problem of the disclosure and use of medical data that are ultimately irrelevant to a specific action.

A similar issue arose in the context of divorce proceedings of Mr. L.L. during which national courts used documents from his medical records without consent and any appointed medical expert[67]. The ECtHR again established a violation of Article 8 ECHR finding that the interference with the applicant's private life had not been justified in view of the fundamental importance of protecting personal data. It observed that the French courts had referred to the impugned medical report on a subsidiary basis to support their decisions, and, apparently, they could have reached the same conclusion without it.

Finally, in the case of Ms. Z, a Finnish national, the health data were included directly in the judgment[68]. Ms. Z and Mr. X (her husband) were both seropositive when X was convicted of rape. Ms. Z's confidential medical records disclosing her infection were seized by the prosecution and included in the investigation file without her prior consent. The City Court held the trial *in camera* and ordered the

66 Judgment of ECtHR of 29 June 2006 on the case of Panteleyenko v. Ukraine, application no. 11901/02.

67 Judgment of ECtHR of 10 October 2006 on the case of L.L. v. France, application no. 7508/02.

68 Judgment of the ECtHR of 25 February 1997 on the case of Z. v. Finland, application no. 22009/93.

ten-year confidentiality period of the case file, but Ms. Z's identity and health data (HIV-status) were published in the final judgment.

The ECtHR agreed that the seizure of the medical records in question and the orders requiring Ms. Z's medical advisers to give evidence in proceedings did not constitute a violation of Article 8 ECHR. However, the ECtHR noted that the national court was informed by X's lawyer about her confidentiality wishes and the lack of consent to the disclosure of information. Further, the ECtHR did not find any cogent reasons which would support the impugned publication of her health data in X's criminal conviction (irrespective of whether she had expressly requested the Court of Appeal not to disclose her identity and medical condition). Accordingly, the ECtHR established that the publication of the information concerned constituted the violation of the right to respect for private life under Article 8[69].

The above discussed cases help to demonstrate that health data processing and unjustified disclosure often take place against the individuals' will and may have irreversible adverse consequences. This kind of disclosure can happen notwithstanding appropriate procedural safeguards. The privacy breach is even more disturbing then, because individuals concerned have confidence that their rights will be respected.

Finally, discrimination based on health concerns both state citizens and foreigners. The ECtHR case-law shows the unequal treatment of migrants in the present context.

2.6. Lesson 5: The misuse of health data of and discrimination against migrants

Our last example concerns the Russian authorities' refusal to grant a residence permit to an Uzbek national because of a seropositive test, in response to which the ECtHR strongly condemned the stigmatization of people living with HIV[70]. Mr. Kiyutin challenged the decision as disruptive of his right to enjoy family life and disproportionate to the legitimate aim of public health protection. The ECtHR stated that the extremely intimate and sensitive nature of the information related to HIV-status calls for the most careful judicial scrutiny of any action taken by states, especially to communicate or disclose such information without consent. While eventually accepting that the impugned measure pursued the legitimate aim of protecting public health, it nevertheless established a violation of Article 14 (prohibition of discrimination) in conjunction with Article 8 ECHR. It also explained that health experts and international bodies recommend that any travel restrictions

69 See also A. Grzelak, Ochrona, *op. cit*., p. 111.

70 Judgment of ECtHR of 10 March 2011 on the case of Kiyutin v Russia, application no. 2700/10.

for seropositive persons cannot be justified by reference to public-health concerns[71]. In these migration cases, the ECtHR also acknowledged that the protection of personal data, including health information, is fundamentally important to the enjoyment of the right to respect for private life guaranteed by Article 8 and freedom from discrimination provided by Article 14 ECHR.

In sum, respect for health data confidentiality is a central aspect of personal privacy in the European human rights system and ought to constitute a vital principle in the legal systems of all members of the Council of Europe. It can be limited under the enumerated exceptions and strict conditions only[72].

Yet, the above-described jurisprudence also demonstrates that a high threshold of health data protection does not decrease the likelihood of disrespect of the existing protection guarantees and the resulting infringements of human rights. This legal-historical analysis serves as a crucial warning of the high temptation of all actors who have access to misuse health data, because health belongs to the most valuable and intimate aspect of human personality. The use of digital tools also prompts additional risks for health privacy[73]. Epidemics of infectious diseases also cause societal fear, which increases the probability of discrimination and stigmatizing practice. In such circumstances, overreactions are likely regardless of established laws.[74]

For these reasons, the regulation and use of Covid-19 applications require a very careful scrutiny of human rights arguments, rule of law principles, and ethical values (public health ethics) to verify whether their development and use can be justified in the aim of preventing disease spread (public health protection). We turn to these arguments in the next section.

3. Public Health Ethics and Covid-19 Digital Applications in Poland: Arguments Against

The analysis will now proceed to the examination of the regulation and exploitation of Covid-19 digital applications in the Polish context (section 2 above)

71 The ECtHR repeated these findings in the judgement of ECtHR of 15 March 2016 on the case of Novruk and others v. Russia, applications nos. 31039/11, 48511/11, 76810/12, 14618/13 and 13817/14.

72 Judgment of ECtHR of 17 January 2012 on the case of Varapnickaitė-Mažylienė v. Lithuania, application no. 20376/05, § 44.

73 Cf. also W.K. Mariner, Mission Creep: Public Health Surveillance and Medical Privacy, "Boston University Law Review" 2007, vol. 87, pp. 347–395, for the U.S. context.

74 See also W.K. Mariner, G.J. Annas and L.H. Glantz, Jacobson v Massachusetts: It's Not Your Great-Great-Grandfather's Public Health Law, "American Journal of Public Health" 2005, vol. 95, Issue 4, p. 587. Cf. C. McClain, Of Medicine, Race, and American law: The Bubonic Plague Outbreak of 1900, "Law and Social Inquiry" 1988, no. 13, pp. 447–513.

through the lens of public health ethics[75]. This lens prompts a closer look at the use of these applications *from the standpoint of three angles*: (i) the protection of human rights and other societal values; (ii) the respect for rule of law, including the focus on health and data protection laws; and (iii) the respect for some ethical principles. In this section, we present our arguments from these three perspectives and embedded in the current Polish reality.

3.1. The Human Rights-Based Arguments and Societal Values

Let us begin by considering the use of applications in Covid-19 prevention in Poland in light of the requirements of human and constitutional rights protection and the related threats of infringements.

First, the case-law histories regarding infectious diseases (see section 3, above) indicate that health data can be easily used without consent, transferred to other, public and private third parties, or misused in employment, administrative and judicial proceedings. Health data in the present context are prone to infringements, because they are predominantly sensitive, since they concern the lives of individuals endangered by a contagion. Further, the societal fear of Covid-19 infection can be simply amplified and lead to devastating social implications of discrimination and exclusion (e.g., children, migrants, and persons with disabilities). These phenomena also often target societal groups, who are already vulnerable, discriminated and/or excluded. As a result, "grey zones" of entire groups avoiding healthcare are likely to occur and lead to the counter-effectiveness of the measures.

Consequently, the protection of individual privacy *and* community public health interests requires recognition of two issues: (i) the vulnerability, caused by infection, of persons already experiencing a disease; and (ii) the devastating character of consequences of breaches of medical confidentiality, including stigmatization and the exposition to "*opprobrium and the risk of ostracism*"[76]. Otherwise, measures claimed to protect public health can become tools of oppression, which are counter-productive to public health protection[77]. It stems from the above-examined cases that courts often included the assessment of these issues in their proportionality analysis.

Second, respect for human (and constitutional) rights in the use of Covid-19 applications arguably requires inclusion of three related aspects of state obligations: respect of individual rights (e.g., privacy), protection from harm from external sources and third parties (standards including necessity and proportionality conditions), and

75 See fn. 15 above.

76 The ECtHR in cases Z v. Finland, *op.cit.*, points 95–96; Biriuk v. Lithuania, *op.cit*, point 36; and Judgment of ECtHR of 6 October 2009 on the case of C. C. v. Spain, application no. 1425/06, point 31.

77 W.E. Parmet, Dangerous Perspectives. The Perils of Individualizing Public Health Problems, "Journal of Legal Medicine" 2009, vol. 30, no. 1, pp. 83–108.

fulfilling the health needs of the population[78]. This means that any possible limitation of health data privacy in the use of digital applications must effectively ensure the high threshold of both constitutional and human rights protection standards (CFR and ECHR), including narrowly interpreted exceptions applied (from the national health law/GDPR) *and* the burden of proof justifying the usefulness of solutions in light of scientific and epidemiological evidence. In light of the analyzed judgments, it would require proving that data collected via Covid-19 applications actually help to reduce the spread of disease effectively; and, further, explaining if, why, and under what conditions, and on what legal basis, they will be used for other purposes (e.g., statistical and research purposes), especially as the latter does not necessarily contribute to the aim of public health protection from the disease.

Third, the protection of collective public health through the use of applications is not the sole value to be defended. The public health ethics approach requires a parallel protection of human dignity and human rights but also of the principles of equality and non-discrimination.[79] The lack of adequate protection of any of these values affects individuals in all their circumstances, including family, social and employment situations. For example, the violation of health privacy can influence the freedom of movement and family reunion, the right to work (freedom of choice of one's profession and place of work), the right to access public service, and other social security rights. Either the denial of employment or redundancy, based solely on an asymptomatic infection by contagious disease, is a frequent consequence of an access to personal medical data by an employer, leading to discrimination (and stigma) in the work environment.

Forth, "public health" is often employed as a "label" for measures the actual objectives of which are different and endanger human rights and privacy. It concerns, for example, state surveillance of health data for security reasons and/or unknown reasons, including storing of data for an unspecified time. The use of security phrasing in the context of health ("war to fight Covid-19") helps to justify such measures.[80] That is why the access by applications to individual health data may provide powerful and easy tools of manipulation of the freedoms of expression and of the press. It can also allow for the politicization of threats/risk assessments, which means using societal fear of the Covid-19 threat to govern, justify disproportionate restrictions of individual rights, and exercise political control over individuals by

78 Cf. G.J. Annas, W. K. Mariner, (Public) Health and Human Rights, *op. cit*, pp. 132–135.

79 See also M. Domańska, People with Disabilities as a Vulnerable Group. The Concept of Protection of the Rights of Vulnerable Groups, "Białostockie Studia Prawnicze" 2018, Vol. 4, no. 23, pp. 25–34.

80 See C. O'Manique and P. Fourie, Security and Health in the Twenty-First Century (in:) M.D. Cavelty and V. Maure (eds.), The Routledge Handbook of Security Studies, Abingdon/New York 2010. Cf. also A Lakoff, Two Regimes of Global Health, "Humanity" 2010, vol. 1, no. 1, pp. 59–79.

portraying them as societal dangers[81]. An "accidental" broadcasting by the state TV of the Covid-19-test information of a leader of public protests against restrictions of reproductive rights in Poland offers a recent relevant example[82]. The Polish CHR has initiated courts' review of the case[83]. Hence, any health data stored through Covid-19 applications could possibly be misused, in a similar way, as indirectly indicated by the case-law histories.

Finally, a state is obliged to ensure health data protection in both horizontal and vertical relations[84]. The access to users' data by private providers of applications' protocols (Google and Apple) create risk to health privacy, which is impossible to assess at the moment. However, it may suggest that the cost of infrastructure for data protection which would be required to exclude any such possibility questions the very rationality of the investment and development of such digital systems. The related arguments return in the next section.

3.2. The Rule of Law Arguments

The consideration of the use of Covid-19 applications in light of the modern and dynamic concept of the rule of law[85] prompts the following observations. They indicate that the development and use of Covid-19 applications might not meet some of the required conditions.

The rule of law requires the limitation of any arbitrary political power, assurance of legal certainty and predictability, and protection of individual and collective human rights from arbitrary actions of public authorities. It also demands that the legal system guarantee a set of standards (mandatory elements): generality, clarity and publicity of norms, no retrospective effect, feasibility, stability, consistency and compliance with the principle of proportionality[86]. When applying these standards to Covid-19 applications in Poland, several significant problems can be identified.

---

81 W.E.Parmet, Dangerous Perspectives, *op. cit*.

82 Marta Lempart on leading Poland's abortion rights protests, 'Financial Times', 02.12.2020, https://www.ft.com/content/b6012449–0c11–419a-b439–6e3320f47e86 (accessed 29.04.2021).

83 Disclosure of the test for SARS-CoV–2 by Marta Lempart – complaint of the Polish Ombudsman to the Provincial Administrative Court, 18.2.2021, https://www.rpo.gov.pl/pl/content/sprawa-ujawnienia-przez-panstwo-testu-na-sars-cov-2-marty-lempart-skarga-rpo-do-wsa (accessed 29.04.2021).

84 Judgment of the Constitutional Tribunal of 19 February 2002, U 3/01, OTK 2002 no. 1A, item 3, para. 1 in fine.

85 See recently: T. Drinóczi and A. Bień-Kacała (eds.), Rule of Law, Common Values, and Illiberal Constitutionalism. Poland and Hungary within the European Union, Abingdon/New York 2020; among the vast literature on the topic; and also W.K. Mariner, G.J. Annas and W. Parmet, Pandemic Preparedness; A Return to the Rule of Law, "Drexel Law Review" 2009, vol. 1, no. 2, pp. 341–382.

86 As there is no opportunity to explain the concept of the rule of law here, one should refer to the documents of international organizations, including the Council of Europe, (2011), The Rule Of Law, adopted by the Venice Commission (CDL-AD(2011)003rev) or the European Commission,

Firstly, the laws establishing Covid-19 applications are not embedded in the Polish health law system in a coherent way. Both applications STOP COVID – ProteGO Safe and Kwarantanna domowa were based on emergency laws enacted in response to the pandemic, which affected their quality, predictability and certainty (see section 2, above).

Moreover, the scrutiny of the Polish applications in use during the pandemic against the requirements of the GDPR general principles deepens the doubts. Michałowicz claims that the terms and conditions of use of the Kwarantanna domowa application and the privacy policy of the ProteGO Safe application are equally not free from textual errors and inconsistencies. They either omit some information required by law or contain contradictory information. For example, these documents indicate that the user may exercise the right to object to the processing of personal data pursuant to Article 21 GDPR, but the exercise of this right is not applicable, because data processing is not based on an appropriate legal basis (arguably, it would need to be Article 6(1), letters e) and f) GDPR)[87]. It can thus be claimed that, because of the health data's sensitive character and the purpose of the applications, data processing in both Covid-19 applications should include a reference to the GDPR's two specific legal bases: Article 6(1), letters e) and f) [88] *and* Article 9(1), letter i) jointly[89]. The next question also arises whether the implementation of the transparency principle – as required by the GDPR – is adequate (Article 5(1), letter a) GDPR).

In summary, the doubts regarding the assessment of Covid-19 applications in light of the GDPR requirements regard data collection's legal basis and purpose (unclear, predetermined purpose for collection; it should be limited to the aim of "protecting against serious cross-border threats to health"[90]); data collection

(2014) Communication from the Commission to the European Parliament and the Council. A new EU Framework to strengthen the Rule of Law (COM(2014) 158 final), as well as the relevant jurisprudence of the Court of Justice (including recent cases C-619/18 *Commission v. Poland* or joined cases C-585/18, C-624/18 and C-625/18 A.K.).

87 A. Michałowicz, Stosowanie, *op. cit.*, p. 37.

88 Article 6(1) letter e) refers to the legal requirement – situation when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Article 6(1) letter f) refers to a legitimate interest – situation when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

89 Article 9(1) letter i) refers to the situation when processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law, which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

90 Cf. Art. 9, Section 1, letter i, GDPR.

scope (some collected data are redundant and unnecessary to achieve the goal set for a specific tool); data collection outcomes (a number of entities authorized to access the data whose activities are not related to the pursued goal); personal data retention time in Kwarantanna domowa (the six-year period of data storing since the application's deactivation, hardly justifiable as a time-limit for civil claims[91]) and in ProteGO (imprecise period of data storing, its privacy policy indicates that data will be "*stored no longer than the use of ProteGO Safe, and not longer than required by law and no longer than necessary to achieve the purpose of processing*"[92]).

There is also some disparity between the applications' technical design (which was assessed positively for ProteGO) and their practical functioning. Theoretically, applications cannot collect the geolocation or physical proximity data of the user (via Bluetooth) when the user chooses information and symptom verification functions only, but the contact-tracing function remains available. Yet, Michałowicz argues that the website, from which ProteGO can be downloaded, requires detailed permissions, including access to device location, Bluetooth settings, and network connections. This indicates that the actual scope of personal data processed in the application may actually be wider than the one declared in the privacy policy[93].

Secondly, the lack of a truly independent control over the system of data processing in case of Covid-19 applications causes concerns. The data transfer to an external server (e.g., managed by the Polish Sanitary Inspectorate) can take place only in strictly defined and justified cases (e.g., a confirmed incident of infection). Yet, it cannot be excluded that the Covid-19 applications will lead to the creation of new databases stored on public administration servers or that the applicable law will be modified to change the destination of the already collected data. Such processes are not impossible because they would be in accordance with, for example, the privacy policy of the ProteGO Safe application. It thus seems in this context that the GDPR-based control by the relevant Polish authority (President of the Personal Data Protection Office) is not sufficient to meet the relevant ECHR standards on the control of access to data by certain governmental services[94].

This is arguable, especially in light of the past experience with the actions of public authorities in Poland. There were some alerting signals before the pandemic

91 A. Michałowicz, Stosowanie, *op. cit.*, p. 40.

92 § 3 pkt 10 ProteGO SafePrivacy Policy, https://www.gov.pl/attachment/092a389f-0a09–438f-9532-b04b8c205c7e (accessed 29.4.2021).

93 A. Michałowicz, Stosowanie, *op.cit.*, s. 39.

94 Cf. Judgment of ECtHR of 23 July 2009 on the case of Hachette Filipacchi Associates v. France, application No. 12268/03, where the ECtHR afforded a margin of appreciation to the state requiring adequate protection to individuals against the arbitrariness of the authorities by ensuring judicial control or other independent control system of measures interfering with the rights of an individual (see also Judgment of ECtHR of 7 March 2017 on the case of Polyakova and Others v. Russia, applications Nos 35090/09 et al.

that some serious shortcomings in the data processing systems in Poland already existed[95]. The fact that the government demonstrated openness to the societal control during the development of the ProteGO Safe application[96], but not with the second one (Kwarantanna domowa), may exactly indicate the change of approach.

The problem with the legal basis for the transfer of data by state authorities has also emerged in several specific situations. For example, in Poland in 2020, presidential elections were to be organized by postal ballots because of the pandemic. Despite the lack of legal acts regulating it, the Minister of Digital Affairs decided to transfer to Poczta Polska (the Polish Post, which was potentially responsible for sending election packages) the data of all citizens entitled to vote. The unlawfulness of the data transfer was confirmed by the Provincial Administrative Court[97]. Second, the governmental actions of pandemic management, based on the Prime Minister's orders solely[98] and the adoption of normative acts of a sub-statutory rank in place of law statutes[99], did not help to overcome the distrust of the digital measures. Given the doubts surrounding the applications against the GDPR requirements outlined above, it is therefore hard to trust and ascertain that the data collected via Covid-19 applications will be used solely for the purposes declared by the authorities.

Lastly, the requirement for the social acceptance of norms belongs to the rule of law conceptualization[100]. Thus, the consideration of three facts is needed in the present context: the high polarization of the Polish society; the overwhelming lack of trust in the government; and the conviction of part of the society that the authorities are moving towards an authoritarian regime[101]. It is not our goal to determine their actuality and extent, but such social beliefs may result in a very low level of acceptance of any solutions that rely on gathering information about society, which

95 Expert team of the Polish CHR, "Osiodłać pegaza" report, September 2019, https://www.rpo.gov.pl/pl/content/osodlac-pegaza-inwigilacja-propozycja-niezalezna-instytucje-do-nadzoru-sluzb-specjalnych (accessed 29.4.2021).

96 Report from the audits of the ProteGO Safe, https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport (accessed 29.4.2021). There is no such report in relation to "Kwarantanna domowa".

97 Judgment of the Provincial Administrative Court in Warsaw of 26 February 2021, IV SA / Wa 1817/20, Lex no. 3150569.

98 Koronawrius. Czy premier nakazał telekomom przekazywanie danych lokalizacyjnych osób chorych i w kwarantannie, 17.4.2020, https://www.rpo.gov.pl/pl/content/koronawrius-rpo-czy-premier-nakazal-przekazywanie-danych-lokalizacyjnych or Do rządu popłynął strumień danych o lokalizacji osób poddanych kwarantannie, 16.4.2020, https://www.rp.pl/Koronawirus-SARS-CoV–2/200419545-Do-rzadu-poplynal-strumien-danych-o-lokalizacji-osob-poddanych-kwarantannie.html (accessed 29.4.2021).

99 For example, the law ordering the wearing of masks was adopted only on October 28, 2020, prior to which this obligation resulted from the provisions of the Regulation of the Council of Ministers only.

100 See note 82 above.

101 W. Sadurski, Poland's Constitutional Breakdown, Oxford 2019.

clearly affects the utility of any such tools. This brings us to the ethical arguments against the applications.

3.3. The Ethical Arguments

Finally, reflecting on the ethical principles and the use of Covid-19 applications provokes several remarks.

The ethical scholarship usually emphasizes that the following principles need to be respected in the use of digital applications in response to the Covid-19 pandemic: autonomy, utility, voluntarism, and equality. The principle of autonomy requires prioritization of individual consent and the citizens' first approach in data protection. In light of the preceding analysis, it is not convincing that both Covid-19 applications respect these principles. Although, theoretically, all grounds of processing personal data are equal, this does not mean that they can be used freely, since different consequences are linked to various legal bases[102]. Imposing a legal basis in the form of a legal obligation would be an expression of the authority and would ignore the ethical aspect and the necessity to take into account the citizens' first approach. In this sense, consent should be a priority for data processing in situations such as those discussed in this text.

Next, the Polish applications can also be questioned from the perspective of the utility principle given the very low number of participants in the ProteGO Safe application, while, in case of Kwarantanna domowa, the relevant data are unknown (see section 2, above). The utility of the tools is doubtful, because usually at least a sixty percent uptake is needed for their effectiveness. Thus, the public usage of mobile applications depends not only on the perfection of technical solutions used in the development of such applications (or potential compatibility of measures with the human rights and constitutional standards, for that matter), but also on the level of social trust and acceptance of far-reaching digitalization to reduce the pandemic (reflected in the number of people using a specific application).

In addition, the Kwarantanna domowa application has not respected the ethical principle of voluntarism entirely. It seems to follow a paternalistic approach in heath law, which should instigate a broader debate that links (public health) ethics and law. Otherwise, the risk of an uncritical acceptance of solutions unjustifiably limiting individual rights increases.

Finally, although the vast majority of the population owns a smartphone, the actual realization of the equal access principle can be questioned. Many persons can encounter the problems with inadequate operation systems on their phones, which do not allow for the applications to be downloaded or encounter difficulties handling them (the elderly, people with disabilities).

102 W. Kotschy, Comment on Article 6, in: Ch. Kuner, L. A. Bygrave and Ch. Docksey (eds.), The EU General Data Protection Regulation (GDPR). A commentary, Oxford 2020, p. 339.

To sum up, in light of the three perspectives applied in this section to examine the design, use and regulation of Covid-19 applications in Poland, it is difficult to conclude that their regulation and use meet fully the requirements of public health ethics based on the protection of human rights, the respect for the rule of law and ethical principles.

Conclusions

This article scrutinizes the normative framework and use of Covid-19 digital applications in Poland and arrives at the conclusion that the implementation of these solutions has not been sufficiently justified. To determine this conclusion, we analytically examine the technical and legal features of the applications; explore the case-law history concerning the potential conflict between the protection of the right to health privacy and public health with the implications for diverse human/constitutional rights; and inspect the applications against the human rights-based standards, ethical principles and the rule of law arguments (the conceptualization of the public health ethics). The article questions the use of these digital tools as such amidst the doubts surrounding them, and, therefore, departs from the approach employed by many existent scholarly works offering analyses of lawful usage of public health surveillance technologies, including coronavirus applications, but usually not questioning the developed solutions[103].

It needs to be emphasized strongly that we do not question the necessity of contact-tracing measures employed by public health authorities during health emergencies/pandemics to identify sources of contagion, inform people about their possible exposure to infection, and impose quarantines to limit the spread of diseases and protect populations' health. The employment of the public health measures can then lead to limiting human/constitutional rights on the condition that at minimum they are lawful and proportionate. However, after scrutinizing the Covid-19 applications in the present text, we see no sufficient safeguards that promise that these conditions will be always fulfilled and individual human rights and data protection will be respected; that third parties will not misuse the data; that the government will actually fulfil its obligations to ensure that no violations occur; or that ethical principles will be followed. Accordingly, we argue that the *digital methods* employed to achieve public health goals must always be examined very carefully, because their justification in terms of a useful prevention of disease spread can likely be unsatisfactory.[104]

103 Cf. S. Sekalala, S. Dagron, L. Forman and B.M. Meier, Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis, "Health and Human Rights Journal" 2020, vol. 22, no. 2, pp. 7–20.

104 Cf. W.K. Mariner, Reconsidering Constitutional Protection, *op. cit.*, p. 1052.

We also think that the purely legal standpoint and analyses are not sufficient to adequately assess the justification of digital applications used for public health purposes. That is why, the application of the critical lens of public health ethics is helpful. It allows for the presentation of a broader picture from the wide-ranging perspectives and the development of a complete and coherent argument around the use of these applications in response to pandemics. In light of the applied lens, our extensive analysis of the Covid-19 applications developed in Poland prompts the recommendation that there is no convincing justification for their use in the present circumstances.

The number of actual threats to the protection of individual rights, including the health privacy, legal reservations and ethical doubts highlighting societal resistance, which *de facto* cannot be feasibly eliminated, do not convincingly outweigh any potential benefit from the use of the applications, at least in light of the analyzed examples. Finally, digital tools can be developed for public health protection, but the key question must always be asked critically: what is their justification?

REFERENCES

Alston P., Does the past matter? On the origins of human rights, "Harvard Law Review" 2013, vol. 126, no. 7.

Annas G.J. and Mariner W.K., (Public) Health and Human Rights in Practice, "Journal of Health Politics, Policy and Law" 2016, vol. 41, no. 1.

Annas G.J., Worst Case Bioethics, Oxford/New York 2011.

Aplikacja „Kwarantanna domowa" budzi wątpliwości obywateli. Rzecznik pisze do premiera, 13.11.2020, https://www.rpo.gov.pl/pl/content/rpo-do-premiera-aplikacja-kwarantanna-domowa-budzi-watpliwosci.

Bradford L. Aboy M. and Liddell K., COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes, "Journal of Law and the Biosciences" 2020, vol. 7, no. 1.

Chałubińska-Jentkiewicz K. and Nowikowska M., Bezpieczeństwo, tożsamość, prywatność – aspekty prawne, Warsaw 2020.

Commission Implementing Decision amending Implementing Decision (EU) 2017/253 as regards alerts triggered by serious cross-border threats to health and for the contact tracing of passengers identified through Passenger Locator Forms, 25.03.2021, no ref. yet.

Communication from the Commission to the European Parliament and the Council. A new EU Framework to strengthen the Rule of Law (COM(2014) 158 final).

Coronavirus contact tracing reignites Polish privacy debate, "Deutsche Welle", https://www.dw.com/en/coronavirus-contact-tracing-reignites-polish-privacy-debate/a-53600913.

Coronavirus Pandemic In The EU – Fundamental Rights Implications: With A Focus On Contact-Tracing Apps, 21 March – 30 April 2020, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf.

COVID-19 App, https://worldhealthorganization.github.io/app.

Dąbrowska-Kłosińska P., Stosowanie unijnych przepisów o transgranicznych zagrożeniach dla zdrowia, a ochrona danych osobowych w UE, „Przegląd Prawa i Administracji Acta Universitatis Wratislaviensis" 2016, vol. 107.

Dąbrowska-Kłosińska P., Tracing Individuals under the EU Regime on Serious, Cross-border Health Threats: An Appraisal of the System of Personal Data Protection, 'European Journal of Risk Regulation' 2017, vol. 8, no. 4.

De Hert P. and Gutwirth S., Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, (in:) S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), Reinventing Data Protection?, Dordrecht 2009.

Deloitte, Privacy and Data Protection in the age of COVID-19, https://www2.deloitte.com/content/dam/Deloitte/be/ Documents/risk/be-risk_privacy-and-data-protection-in-the-age-of-covid-19.pdf.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (O.J. L 119, 4.5.2016).

Disclosure of the test for SARS-CoV–2 by Marta Lempart – complaint of the Polish Ombudsman to the Provincial Administrative Court, 18 February 2021, https://www.rpo.gov.pl/pl/content/sprawa-ujawnienia-przez-panstwo-testu-na-sars-cov-2-marty-lempart-skarga-rpo-do-wsa.

Do rządu popłynął strumień danych o lokalizacji osób poddanych kwarantannie, 16.4.2020, https://www.rp.pl/Koronawirus-SARS-CoV–2/200419545-Do-rzadu-poplynal-strumien-danych-o-lokalizacji-osob-poddanych-kwarantannie.html.

Domańska M., People with Disabilities as a Vulnerable Group. The Concept of Protection of the Rights of Vulnerable Groups, "Białostockie Studia Prawnicze" 2018, vol. 4, no. 23.

Drinóczi T., Bień-Kacała A. (eds.), Rule of Law, Common Values, and Illiberal Constitutionalism. Poland and Hungarywithin the European Union, Abingdon/New York 2020.

eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19, Common EU Toolbox for Member States, https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

European Commission, Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, 2020/C 124 I/01, C/2020/2523 (O.J. C 124I, 17.4.2020).

European Data Protection Board (EDPB), Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21.4.2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

European Data Protection Supervisor (EDPS), EU Digital Solidarity: a call for a pan-European approach against the pandemic, 06.4.2020, https://edps.europa.eu/sites/edp/files/publication/2020–04-06_eu_digital_solidarity_covid19_en.pdf.

Expert team of the Polish CHR, "Osiodłać pegaza" report, September 2019, https://www.rpo.gov.pl/pl/content/osodlac-pegaza-inwigilacja-propozycja-niezalezna-instytucje-do-nadzoru-sluzb-specjalnych (accessed 29.4.2021).

Florczak-Wątor M., Komentarz do art. 51 Konstytucji, (in:) P. Tuleja (ed.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warsaw 2020.

FRA and Council for Europe, Handbook on European Data Protection Law, Luxembourg 2018.

Fundamental Rights Agency, Coronavirus Pandemic in the EU – fundamental rights implications: with a focus on contact-tracing apps, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf.

Garlicki L. and Zubik M. (eds.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, Tom I, Warsaw 2016.

Grzelak A. (ed.), Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Warsaw 2019.

Grzelak A., Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości, Warsaw 2015.

Jackowski M., Ochrona danych medycznych, Warsaw 2011.

Joined statement on the right to data protection in the context of the COVID-19 pandemic by A. Pierucci and J.-P. Walter, 30.3.2020 https://rm.coe.int/covid19-joint-statement/16809e09f4.

Kędzior M., The right to data protection and the COVID-19 pandemic: the European approach, 'ERA Forum' 2021, no. 21.

Koronawrius. Czy premier nakazał telekomom przekazywanie danych lokalizacyjnych osób chorych i w kwarantannie, 17.4.2020, https://www.rpo.gov.pl/pl/content/koronawrius-rpo-czy-premier-nakazal-przekazywanie-danych-lokalizacyjnych.

Koschalka B., Uptake of Covid contact tracing app under 2% in Poland, among the lowest rates in Europe, 11.9.2020, https://notesfrompoland.com/2020/09/11/uptake-of-covid-contact-tracing-app-under-2-in-poland-among-the-lowest-rates-in-europe.

Kotschy W., Comment on Article 6, (in:) Ch. Kuner, L.A. Bygrave and Ch. Docksey (eds.), The EU General Data Protection Regulation (GDPR). A commentary, Oxford 2020.

Kusat Kaya E., Safety and privacy in the time of covid-19: contact tracing applications, https://www.jstor.org/stable/resrep26089?seq=1#metadata_info_tab_contents.

Lakoff A., Two Regimes of Global Health, "Humanity" 2010, vol. 1, no. 1.

Łakomiec K., Konstytucyjna ochrona prywatności. Dane dotyczące zdrowia, Warsaw 2020.

Lucivero F., Hallowell N., Johnson S., Prainsack B., Samuel G. and Sharon T., COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale, "Journal of Bioethical Inquiry" 2020, no. 17.

Mariner W.K., Annas G.J. and Glantz L.H., Jacobson v Massachusetts: It's Not Your Great-Great-Grandfather's Public Health Law, "American Journal of Public Health" 2005, vol. 95, Issue 4.

Mariner W.K., Annas G.J. and Parmet W., Pandemic Preparedness; A Return to the Rule of Law, "Drexel Law Review" 2009, vol. 1, no. 2.

Mariner W.K., Mission Creep: Public Health Surveillance and Medical Privacy, "Boston University Law Review" 2007, vol. 87.

Mariner W.K., Reconsidering Constitutional Protection for Health Information Privacy, "Journal of Constitutional Law" 2016, vol. 18, no. 3.

Marta Lempart on leading Poland's abortion rights protests, "Financial Times", 02.12.2020, https://www.ft.com/content/b6012449–0c11–419a-b439–6e3320f47e86.

MC zapewnia: aplikacja mobilna „Kwarantanna Domowa" - zgodna z wymogami RODO, 30.11.2020, https://www.rpo.gov.pl/pl/content/mc-zapewnia-rpo-aplikacja-kwarantanna-domowa-zgodna-z-rodo.

McClain C., Of Medicine, Race, and American law: The Bubonic Plague Outbreak of 1900, "Law and Social Inquiry" 1988, no. 13.

Michałowicz A., Stosowanie aplikacji mobilnych podczas pandemii COVID-19 z perspektywy ochrony danych osobowych, „Europejski Przegląd Sądowy" 2020, no. 6.

Murphy T., Health and Human Rights' Past: Patinating Law's Contribution, "Health and Human Rights Journal" 21 November 2019.

Norwegian Infection Stop, https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps.

O'Manique C. and Fourie P., Security and Health in the Twenty-First Century (in:) M.D. Cavelty and V. Maure (eds.), The Routledge Handbook of Security Studies, Abingdon/New York 2010.

O'Neill P.H., Ryan-Mosley T. and Johnson B., A flood of coronavirus apps are tracking us. Now it's time to keep track of them, "MIT Technology Review", 7 May 2020, https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker.

Obem A., ProteGO Safe: instalować czy nie?, 3.8.2020, https://panoptykon.org/czy-instalowac-protego-safe.

OECD Policy Responses to Coronavirus (COVID-19), Ensuring data privacy as we battle COVID-19, 14.4.2020 http://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19–36c2f31e/#section-d1e690.

Pagliari C., The ethics and value of contact tracing apps: International insights and implications for Scotland's COVID-19 response, "Journal of Global Health" 2020, vol. 10.

Parmet W.E., Dangerous Perspectives. The Perils of Individualizing Public Health Problems, "Journal of Legal Medicine" 2009, vol. 30, no. 1.

Privacy leaders, https://iapp.org/resources/article/privacy-leaders-views-impact-of-covid19-on-privacy-priorities-practices-programs.

Protection of health-related data – Recommendation CM/Rec(2019)2 adopted by the Committee of Ministers of the Council of Europe, 27.3.2019.

Ram N. and Gray D., Mass surveillance in the age of COVID-19, "Journal of Law and the Biosciences" 2020, vol. 7, no. 1.

Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (O.J. L 119, 4.5.2016).

Report from the audits of the ProteGO Safe, https://www.gov.pl/web/protegosafe/audyt-bezpieczenstwa--zobacz-raport.

Report of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, 3.8.2018, https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx.

Report on the rule of law - Adopted by the Venice Commission at its 86th plenary session, Venice, 25–26 March 2011.

Roberts S.L., Big Data, Algorithmic Governmentality and the Regulation of Pandemic Risk, "European Journal of Risk Regulation" 2019, vol. 10, Issue 1.

Rojszczak M., Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa autorytarnego, „Acta Universitatis Wratislaviensis - Studia nad Autorytaryzmem i Totalitaryzmem" 2020, vol. 42, no. 2.

Rojszczak M., Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji, Warsaw 2019.

Sadurski W., Poland's Constitutional Breakdown, Oxford 2019.

Safjan M., Bosek L. (eds.), Instytucje Prawa Medycznego. System Prawa Medycznego. Tom 1, Warsaw 2017.

Safjan M., Bosek L. (eds.), Konstytucja RP. Tom I. Komentarz do art. 1–86, Warsaw 2016.

Sekala S., Dagron S., Forman L., and Meier B.M., Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis, "Health and Human Rights Journal" 2020, vol. 22, no. 2.

Sroka T., Ograniczenia praw i wolności konstytucyjnych oraz praw pacjenta w związku z wystąpieniem zagrożenia epidemicznego, „Palestra" 2020, no. 6.

Świtała K., Interoperacyjność i bezpieczeństwo danych medycznych w systemach e-zdrowia i telemedycynie, (in:) I. Lipowicz, M. Świerczyński and G. Szpor (eds.), Telemedycyna i e-Zdrowie. Prawo i informatyka, Warsaw 2019.

Theme 3: Covid-19, privacy rights and cyber security risks, 'Covid-19 Resources', Pinciples for Responsible Investment, 7.9.2020, https://www.unpri.org/covid-19-resources/theme-3-covid-19-privacy-rights-and-cyber-security-risks/6343.article.

There's an app for that: Coronavirus apps, 20.4.2020, https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps.

Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics, 23.4.2020, OECD, https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636.

Tuleja P., Komentarz do art. 31 Konstytucji RP, (in:) P. Tuleja (ed.), Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warsaw 2020.

Van Kolfschooten H. and de Ruijter A., COVID-19 and privacy in the European Union: A legal perspective on contact tracing, "Contemporary Security Policy" 2020, vol. 41, Issue 3.

Van Zeben J. and Kamphorst B.A., Tracking and Nudging through Smartphone Apps: Public Health and Decisional Privacy in a European Health Union, "European Journal of Risk Regulation" 2020, vol. 11, Issue 4.

Wałachowska M., Ochrona danych osobowych w prawie cywilnym i medycznym, Toruń 2008.

Wiewiórowski W.R., Profilowanie osób na podstawie ogólnodostępnych danych, (in:) A. Mednis (ed.), Prywatność a ekonomia: ochrona danych osobowych w obrocie gospodarczym, Warsaw 2013.

Wiewiórowski W.R., Rola Unii Europejskiej w koordynacji zastosowania narzędzi informatycznych do walki z pandemią, „Europejski Przegląd Sądowy" 2020, no. 6.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.05

Received: 12.02.2021
Accepted: 10.05.2021

Anetta Breczko
University of Bialystok, Poland
breczko@uwb.edu.pl
ORCID ID: https://orcid.org/0000–0003-4856–5396

Human Enhancement in the Context of Disability (Bioethical Considerations from the Perspective of Transhumanism)

Abstract: In the present paper we examine several problems associated with medical development in the field of human-enhancing technologies, particularly with respect to disability. The subject of our considerations partly focuses on the fact that progress in biotechnology and information technology in medicine has contributed to the elimination of diseases and various health disorders (including some aspects of disability). Furthermore, we centre our attention on the dilemma of increasing the efficiency and activity of those who are 'fully functional', by introducing, among others, the available exo-extensions (such as exo-prostheses), endo-implantation and reprogenetics (such as PDG and CRISPR methods). Finally, we point out several ethical and legal doubts surrounding the apparent intention of creating a transhumanist vision of the 'perfect human being' ('post-human', 'bionic human', 'human cyborg').
Keywords: disability, eugenics, health, human enhancement, quality of life, transhumanism,

Introduction

The mission of medicine is identified with care for the patient's health, in accordance with the principle *salus aegroti suprema lex*, well grounded in both the law and ethics. The traditional purpose of medicine is to treat the ill and ailing. It is achieved with the available pharmacological and surgical means, and with appropriate rehabilitation. In situations where therapy becomes futile, the most important task is to provide appropriate palliative care. It should be mentioned that the classic mission of medicine is linked with health-promoting education. With progress in biotechnology, information technologies and artificial intelligence,

the actions of physicians begin to focus on the 'improvement' ('correction') of the human condition. Aside from therapeutic activities, special importance is currently associated with non-therapeutic 'human enhancement' procedures. Physical condition can currently be improved with different enhancements (so-called exo-extensions and endo-extensions). The brand-new and very controversial methods applied in this area include the brain–computer interface, which became possible thanks to biomedical and computer methods.[1] Prevention of disability has been made possible, many years ago, with genetic eugenics (so-called *reprogenetics*).[2] One of the most important tools in this area is Pre-implantation Genetic Diagnostics (PGD).[3] Recent years have also brought huge hopes associated with the so-called CRISPR method.[4]

The technological capabilities of contemporary medicine allow not only restoring ability to disabled persons but also significantly extending it, sometimes resulting in the transformation of a disabled person towards *super-ability*.[5] The available biotechnology instruments and tools have therefore created real opportunities for the improvement of human genetic potential and physical, mental and intellectual well-being, but also for improvement in the quality of life of societies on the global scale. The new methods for improvement of physical, mental and even emotional conditions are, however, associated with numerous controversies of a philosophical, moral and legal nature. These disputes cover, for instance, the understanding of human nature. Numerous doubts are associated with potential threats to the dignity, integrity, identity, freedom and equality of individuals.[6] Despite the various fears associated with the implementation of technological opportunities, there is huge hope tied to the chance for practical realization of the transhumanistic vision of the 'perfect human' (who is 'super-able') that could be tied to the reduction, or perhaps even elimination, of the problem of disability.

1 M. Klichowski, Narodziny cyborgizacji. Nowa eugenika, transhumanizm i zmierzch edukacji, Poznań 2014, pp. 153–160.

2 J. Domaradzki, Janusowe oblicze reprogenetyki, „Nowiny Lekarskie" 2009, vol. 78, no. 1, pp. 72–73.

3 M. Soniewicka, Selekcja genetyczna w prokreacji medycznie wspomaganej. Etyczne i prawne kryteria, Warsaw 2018, p. 151ff.

4 G. Lindenberg, Ludzkość poprawiona. Jak najbliższe lata zmienią świat, w którym żyjemy, Krakow 2018, pp. 23–49.

5 M. Klichowski, Narodziny cyborgizacji, *op. cit*., pp. 150–153.

6 T. Żuradzki, Nowa liberalna eugenika: krytyczny przegląd argumentów przeciwko biomedycznemu poprawianiu ludzkiej kondycji fizycznej lub umysłowej, „Diametros" 2014, no. 42, p. 208.

1. The Transhumanist Vision of the 'Perfect Human' (the 'Super-able')

The drive towards the creation of the 'perfect human' (which also means 'able-bodied' or even 'super-able') is visible in the ruminations of the transhumanists. The main assumption of this intellectual trend, referred to also as *Humanity plus* (H+), is the symbiosis of *Homo sapiens* with technology, meant to offer humans 'perfection' (super-efficiency) in the near future. According to transhumanist forecasts, the gradual integration of people with modern technological tools would soon make it possible to overcome all biotechnological barriers.[7] According to these predictions, the new 'bionic humans' would live as long as possible and in the best condition possible. In the end, they would start functioning not only as 'able-bodied', but also as super-healthy, super-empathic, super-rational and ultimately even immortal individuals. Finally, one would become a more perfect version of oneself.[8] The transhumanists stress that the contemporary abilities of the human body are nothing exceptional and constitute just one of the phases of evolution. Biotechnology is to make realistic the transfer of humankind to the highest level of evolutionary development. It is through biotechnology that a post-human, technologically enhanced civilization – a civilization of cyborgs – would finally take over control of the universe.

The beliefs of the transhumanists are strictly associated with the concept of *human enhancement*, which is to serve as the basis for the construction of the vision of the 'perfect human'. This idea is tied to the hope that the problem of disability could be completely eliminated some time in the future, or at least significantly reduced. It should be noted that transhumanism is based on a specific interpretation of this idea; it is not the only interpretation, but a very suggestive one. That is why it will become the basis for further considerations of the challenges and ethical dilemmas associated with the restoration of physical ability to disabled persons or indeed with the creation of above-average abilities in people.

The term *human enhancement* literally means the extension or increasing of human abilities. It refers to activities which contribute to positive modifications of human bodily and mental structures and which boost the individual's ability to act. The purpose of these operations is the ultimate improvement of human well-being. Having in mind the available technological solutions, one could conclude that humankind 'as never before faces a whole series of mighty opportunities tied to influencing the life of an individual and the lives of the future generations. Hence the question becomes what these capacities entail, what we can use them for and how

7 The best-known proponents of transhumanism are currently Ray Kurzweil, Hans Moravec, Erich Drexler, Vernor Vinge and Fereidoun M. Esfandiary.

8 K. Szymański, Czy od transhumanizmu można uciec? „Filozofuj! Nowy człowiek?" 2017, vol. 6, no. 18, p. 13.

we can justify these interventions.'[9] In the context of the technological opportunities for supporting the physical and mental condition of humans, the crucial issue seems to be the question regarding the meaning of the term 'health' and other terms associated with it. This will be discussed further on in this paper.

2. Support for the Physical and Mental Condition of Humans in the Context of Understanding the Term 'Health'

'Health' is an exceptionally polysemous concept.[10] From the standpoint of this paper, two approaches seem particularly important: the positive and the negative approaches. The dominant way of understanding the term 'health' is the 'positive' approach, which is reflected in Article 1 of the Constitution of the World Health Organization (WHO) from 1964. It states that 'The objective of the World Health Organization… shall be the attainment by all peoples of the highest possible level of health.' The preamble to the constitution defines this general purpose as the right of every individual: 'The enjoyment of the highest attainable standard of health is one of the fundamental rights of every human being, without distinction of race, religion, political belief, economic or social condition.' Thus, health is defined as the status of well-being – physical, mental and social – and not just the absence of illness and disabilities.[11] This condition enables the individual to adapt to the environment and to fulfill plans and aspirations.[12]

For transhumanists, the manner of defining the term 'health' is most frequently tied to the 'negative' approach. This concept is beginning to be identified with a state of the functioning of the body in which none of the diseases and pathologies known so far has the opportunity to manifest itself. The available medical technologies offer the opportunity to eliminate diseases right at their source.

The context of deliberations on what 'health' really is discloses the vagueness of such terms as, for example, 'normality' or 'happiness'. The relationship of 'full capability' and 'disability' to 'happiness' and 'normality' turns out to be unclear. It can be noted that contemporary democratic societies on the one hand promote the concept of the inclusion of persons with disabilities in social life, believing that such persons can be as happy and productive as 'fully capable' persons. On the other hand, there is the promotion of the 'concept of selective reproduction to counteract

9 G. Hołub (ed.), Ulepszanie człowieka. Fikcja czy rzeczywistość? Argumenty, krytyka, poszukiwanie płaszczyzny dialogu, Krakow 2018, p. 10.

10 There are about 120 definitions; see J. Domaradzki, O definicjach zdrowia i choroby, "Folia Medica Lodziensia" 2013, no. 40, p. 6.

11 Constitution of the World Health Organization, https://www.who.int/governance/eb/who_constitution_en.pdf (accessed 24.03.2021).

12 On interpretation doubts tied to the positive definition of health, see W. Galewicz, Zdrowie jako prawo człowieka, "Diametros" 2014, no. 42, p. 59.

disability, on the basis of the fact that persons with disabilities are, as a rule, less happy than the fully capable ones, which undermines the first assumption.'[13] This is arguably tied to the horizontal incoherence of biolaw, related to the danger of a utilitarian, often highly simplified, moral arithmetic.

An in-depth analysis of the problem referred to above would require separate exploration, reaching well beyond the scope of this paper. It is however undisputed that technological capabilities influence a change in the manner of understanding many terms correlated with the concept of 'health'. Zygmunt Bauman aptly noted this many years ago, analyzing the manner of understanding the categories of 'health' and 'fitness'. He wrote that both these terms 'are often taken to be coterminous and are used synonymously; after all, they both refer to the care of the body, to the state in which one wishes one's body to achieve and the regime which the owner of the body should follow to fulfill that wish. To treat the two terms synonymously is, though, a mistake – and not merely for the well-known fact that not all fitness regimes "are good for one's health" and that what helps one to stay healthy does not necessarily make one fit. Health and fitness belong to two quite different discourses and appeal to very different concerns.'[14]

'Health' should therefore be understood as the proper and desirable state of the human body and spirit that can be more or less exactly described and precisely measured. It refers to a bodily and mental condition that enables the satisfaction of the social role assigned to an individual. 'To be healthy' means in most cases 'to be employable'.[15]

Meanwhile, 'fitness' means being ready to take on challenges which were so far unknown and unpredictable. 'It does not refer to any particular standard of bodily capacity, but to its (preferably unlimited) potential of expansion. "Fitness" means being ready to take on the unusual, the non-routine, the extraordinary – and above all the novel and the surprising. One may almost say that if health is about "sticking to the norm", fitness is about the capacity to break all norms and leave every already achieved standard behind.'[16]

Bauman also points out the fact that health used to be measured with set (countable and measurable) categories, such as bodily temperature or blood pressure. The concept was clear thanks to the distinction between the 'norm' and the 'pathology'. However, nowadays the status of all criteria, including health criteria, is severely undermined and has become very uncertain: 'What yesterday was considered normal and thus satisfactory may today be found worrying, or even pathological and calling for remedy. First, ever-new states of the body become legitimate reasons for medical

13 M. Soniewicka, Selekcja genetyczna, *op. cit.*, p. 197.
14 Z. Bauman, Liquid Modernity, Cambridge 2000, p. 77.
15 *Ibidem*, p. 78.
16 *Ibidem.*

intervention – and the medical therapies on offer do not stay put either. Second, the idea of "disease", once clearly circumscribed, becomes even more blurred and misty.'[17]

To illustrate the 'blurring' of the meaning of such concepts as 'health–disease' and 'fitness–disability', one can use the example of the famous runner Oscar Pistorius, who lost both legs as a baby. Prostheses made of carbon fibre made it possible for him, as a disabled person, not only to return to 'ordinariness' (in terms of health), but also to win major titles in track and field competitions for people with disabilities. Pistorius has also successfully competed against fully fit runners. A doubt has arisen regarding the category in which he should compete: as a healthy person ('able-bodied' or perhaps even 'super-able') or as a 'person with disabilities'?

It is probably not an exaggeration to say that Pistorius has become an ambassador of the idea, mentioned in the introduction, of the transformation of a 'disabled' person into a 'super-able' one. His case clearly contributed to a change in the understanding of the concepts referred to above. It gave the impulse to the doctrinal discussion of the following problem: Do some modern medical technologies really provide a 'repair' (the restoration of health) or perhaps rather an 'improvement' (a correction)?

We should note that the concept of 'therapy' – in its classical understanding – is tied to 'repair' (i.e. the restoration of ordinary health). In the case of Pistorius, the therapy resulted in an 'improvement' (a 'correction'), that is, it led to above-ordinary ability. A person who so far was disabled was given above-ordinary (superhuman?) abilities, demonstrating a higher efficiency (of course, in a certain narrow area) than an 'able-bodied' person.[18] Did he therefore become a 'cyborg'? Michał Klichowski, author of the book *Narodziny cyborgizacji. Nowa eugenika, transhumanizm i zmierzch edukacji* (*The Birth of Cyborgization. The New Eugenics, Transhumanism and the Decline of Education*), believes that 'the strategies of the fight against disability started turning into strategies of cyborgization, the disabled persons became models for cyborgs and super-ability became a phase of transhumanist techno-progress'.[19] Perhaps, as Jerzy Kopania claims, the road to health (defined in the negative manner) shall lead through various forms of cyborgization in terms of quality, 'meaning the gradual replacement of natural organs with artificial ones, connection of the brain to computer systems, controlling bodily processes via external electronics, etc.'[20]

We should not exclude the possibility that further progress in the knowledge and development of biotechnology and information technology will enable continuous and increasingly far-reaching improvement of the physical and spiritual sphere of

17 *Ibidem*, p. 122.

18 M. Klichowski, Narodziny cyborgizacji, *op. cit.*, p. 151.

19 *Ibidem*, p. 152.

20 J. Kopania, Projekt udoskonalenia człowieka w świetle relacyjnej koncepcji osoby, (in:) P. Duchliński and G. Hołub (eds.), Ulepszanie moralne człowieka. Perspektywa filozoficzna, Krakow 2019, pp. 130–131. H. Fry, Jak być człowiekiem w epoce maszyn, Krakow 2018, p. 146.

humans (their 'repair' and 'improvement'). Perhaps with time, as the transhumanists predict, the human body will stop being susceptible to all kinds of ailments, and its strength and ability will reach the maximum possible level. Thus, both the *soma* and the *psyche* of humans would be improved to such a degree that the final result would be 'perfect well-being' or perhaps even eternal life.[21]

3. Practical Implications of Biotechnological Progress in 'Human Improvement' and the Reduction (Elimination?) of the Disability Problem

Despite numerous controversies (such as those mentioned earlier), biotechnological progress nowadays enables practical medical support for the human body on a scale that earlier was unimaginable. Advances in genetics, information technology and artificial intelligence undoubtedly contribute to this. Algorithms have started diagnosing various diseases even under standard medical procedures.[22] Intensive and interdisciplinary research into the processes of ageing and the possibilities to maximize the length of human life is of great practical importance in the development of technologies that support the human body and psyche. Their results are successfully used to 'improve' the life not only of persons with various disabilities but also of 'able-bodied' people.[23] The contemporary technological tools supporting the body and mind justify the statement that 'cyborgization' is no longer something that belongs purely in the science-fiction sphere. It has become contemporary reality. Exo- and endo-extensions are a fact in countries with the highest level of technological development.[24] The possible interventions for restoring ability and fitness to disabled persons or for boosting the natural abilities of a healthy person have been named *Human Enhancement Technologies* (HET).[25] Technologies of this type can be broken down into two primary areas. The first is associated with the bodily aspect of humans, with health and physical fitness. In this case, new technologies can be used for such purposes as monitoring the overall condition of the body, any increase of height or muscle mass, the elimination of faulty genes and the prolongation of life. The second area covers the psyche, including mental, emotional or behavioural ability. Technologies in this area are used to increase the level of intelligence and improve memory capabilities, but also to eliminate aggression.[26]

21 J. Kopania, Projekt udoskonalenia, *op. cit.*, p. 154ff.
22 H. Fry, Jak być człowiekiem, *op. cit.*, p. 154ff.
23 The leading role is played by the California-based company Calico, founded in 2013 by Google and Arthur D. Levinson.
24 M. Klichowski, Narodziny cyborgizacji, *op. cit.*, pp. 150–160.
25 J. Savulescu and N. Bostrom (eds.), Human Enhancement, Oxford 2009, p. 25ff.
26 B. Chyrowicz, Spór o poprawianie natury ludzkiej, Lublin 2004, pp. 47–61.

Let us begin from examples of strengthening the body. Physical fitness is supported with various devices and applications, used on a daily basis, that enable monitoring of the body and, through this, self-control of health (e.g. trackers that count steps, calories or heart rate). Physical fitness can be achieved or improved with such solutions as tooth implants, cochlear implants and endo-prostheses of the hip or knee joints. The attainment, or even improvement, of ability and fitness becomes possible with bionic limbs. The most technologically advanced tools are equipped with artificial intelligence solutions. For example, a myoelectric hand prosthesis is able to recognize various muscle-activity patterns and therefore can be more perfect than an organic hand. To restore health to the human body, various bionic organs are implanted: an artificial liver, heart or kidney, synthetic skin, blood or bones – and recently even a bionic eye. Exoskeletons enable proper body functioning not only for the disabled (e.g. paralyzed persons) but can be used to increase the strength of healthy persons (e.g. soldiers). It can therefore be concluded that bionics and the tools which have been developed have become incredibly helpful, and not only for persons with various disabilities who can use them to restore their fitness and attain relative independence. Bionics can be used to improve and boost the bodily functions of a 'fully healthy' person.

From the point of view of disability considerations, actions involving attempts to eliminate disability play a special role today. Progress in overall genetics is coupled with the intense development of the trend referred to as *genetic enhancement*. It includes the manipulation of human genes, which is frequently very controversial from the ethical and legal standpoint.[27] Concepts of the genetic improvement of humans are associated primarily with *in vitro* fertilization technology (IVF), which offers the opportunity for targeted selection of female and male gametes so as to result in a child with strictly defined physical and genetic characteristics. 'Pre-birth improvement' is based on the assumption that the appearance (or non-appearance) of individuals with certain characteristics and genetic predispositions is desirable. Thus, 'genetic correction' can, first of all, lead to the elimination of genetically faulty embryos. Its purpose is then to not permit the birth of an individual with certain genetic defects (so-called negative eugenics). Pre-implantation Genetic Diagnosis (PGD) is used to eliminate an embryo burdened with the defect. Implanting non-defective embryos in its place (*screening out*) creates a high probability of conception and the birth of a child free of genetic diseases and other defects and issues.[28] In the opinion of the European Court of Human Rights, the right to conceive a healthy

27 O. Nawrot, O zakresie dopuszczalności ingerencji wobec ludzkiego genomu, (in:) A. Białek and M. Wróblewski (eds.), Prawa człowieka a wyzwania bioetyczne związane z nowymi technologiami, Warsaw 2018, pp. 123–142.

28 K. Bączyk-Rozwadowska, Prokreacja medycznie wspomagana. Studium z dziedziny prawa, Toruń 2018, p. 331ff.

child, free from genetic defects and impediments, falls within the sphere of private and family life protected by the Convention for the Protection of Human Rights and Fundamental Freedoms.[29] Prohibiting embryo selection when there is a risk of disease is a disproportionate restriction on this right.[30] Of course, enormous controversy surrounds the work on drafting a catalogue of developmental diseases, including defects leading to disability, that would enable such embryo selection. Some believe that actions of this kind are an attempt at eugenics in its classic, negative meaning, offering the opportunity to eliminate all individuals with any type and degree of dysfunction. They claim that this procedure is a manifestation of undesirable practices, as it enables the selection of embryos due to their 'genetic quality'. PGD is thus seen as a form of eugenic practice that leads inevitably toward the instrumental and commercial treatment of human reproduction.[31]

From the transhumanist perspective, the use of available technologies, including assisted reproduction, to not only eliminate defects but also to strengthen the genetic makeup of a healthy human organism (so-called positive eugenics) is highly advisable. Therefore, genetic correction should also be used to maximize the 'efficiency' of humans. In the opinion of transhumanists, parents actually have a moral duty to guarantee their child the best possible start in life. Therefore, they should use all available genetic knowledge to ensure that their progeny arrives in this world with the best 'equipment' possible.[32] It is noted that the selection of specific characteristics for a child occurs virtually routinely for infertile couples using sperm and egg banks. In these banks, anonymous donors are catalogued according to characteristics such as race, height, eye colour, hair colour, education or even occupation. There is even a sperm bank of Nobel Prize laureates, which specializes in acquiring sperm from outstanding personalities.[33] The procedure of creating so-called *designer babies* is used in IVF practice with the use of genetic material from anonymous donors. There are, however, very significant dangers associated with the technologically possible realization of future parents' subjective ideas about their ideal offspring. It could happen that they would want not only to 'program' a child

29 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), https://www.echr.coe.int/Documents/Convention_ENG.pdf (accessed 25.03.2021).

30 Judgment of the European Court of Human Rights of 28 August 2012 on the case of Costa and Pavan v. Italy, application no. 54270/10.

31 D. King, Preimplantation Genetic Diagnosis and the 'New' Eugenics, "Journal of Medical Ethics" 1999, vol. 25, p. 178.

32 M. Soniewicka, Czemu ulepszanie genetyczne budzi sprzeciw? 'Filozofuj! Nowy człowiek?' 2017, no. 6, pp. 19–21.

33 D. Plotz, Fabryka Geniuszów. Niezwykła historia banku spermy noblistów, Warsaw 2007.

of a defined sex, appearance, character traits, abilities or level of intelligence, but also a child with a defect and impairment that they themselves have, e.g. deafness.[34]

There are also ethical and legal concerns related to, for example, the possibility of tissue typing. In some countries (e.g. Sweden) this is permitted by law. Tissue typing leads to the birth of *saviour siblings*, sometimes also referred to as 'medicine children' (or 'utility children'). The moral imperative prohibiting the instrumental treatment of humans (in this case, a child conceived in order to enable the treatment of another, already-living child) seems to speak against such 'saviour conception'.[35] Some also point to the possibility that with time, the goal of scientists would be to create a 'custom human', adapted to high technology. There is the risk that when typical therapeutic interference with the human genome is permitted, we can overlook the moment when the genetic makeup of a human being becomes changed without any medical justification.

Numerous controversies of a moral and legal character are nowadays tied to so-called gene therapy, which undoubtedly can be used to improve the human condition. Gene therapy is already used to treat certain genetic diseases (such as epidermolysis bullosa) by taking cells from the patient and modifying the faulty DNA segment. In recent years, 'mixing genes' has also become possible, which has led to the creation of so-called chimeras. Their creation has become a common practice in the field of transplantology – two sets of genes in a single human body are today the obvious result of transplantation procedures. Techniques for the modification and editing of genes result in the intensification of bioethical disputes regarding so-called human chimeras. It should be mentioned that children of three parents (children who have genes from two mothers and one father as a result of cytoplasmic transfer into the germline) have already been born. In a 2016 experimental formula of *in vitro* fertilization, performed with the Mitochondrial Replacement Therapy (MRT) technique, an egg cell from the mother, sperm from the father and another egg cell from a donor were used. By developing this method, the scientists wanted to find a way to protect children against mitochondrial diseases inherited from the mother. So far, there are about twenty children born whose mitochondrial DNA is obtained in part from a donor.[36] This leads to questions regarding the potential consequences of having genetic features of different persons.[37]

34 J. Savulescu, Deaf Lesbians, Designer Disability' and the Future of Medicine, "British Medical Journal" 2002, vol. 325, p. 771.

35 M.W. Wolf and J.P. Kahn, Using Preimplantation Genetic Diagnosis to Create a Stem Cell Donor: Issues, Guidelines and Limits, "Journal of Law, Medicine and Ethics" 2003, vol. 31, p. 331ff.

36 L. Tomala, Wywiad z prof. E. Bartnik: Na świecie żyją osoby o zmodyfikowanym DNA, "Nauka w Polsce", http://naukawpolsce.pap.pl/aktualnosci/news%2C80306%2Cprof-bartnik-na-swiecie-zyja-juz-osoby-o-zmodyfikowanym-dna.html (accessed 27.01.2020).

37 M. Leźnicki and A. Lewandowska, Biomedykalizacja a genetyczne udoskonalanie człowieka w kontekście analiz bioetycznych, „Acta Universitatis Lodziensis" 2013, no. 45, pp. 113–129.

A harbinger of previously unimagined genetic possibilities is the CRISPR method, referred to as 'molecular scissors'. It enables interference in the DNA structure much more precisely than ever before and is perceived as an alternative to the genome-editing methods employed so far.[38] Matthew Cobb predicted in 2017 that 'it seems inevitable that the world's first CRISPR baby will be born sometime in the next decade, most likely as a result of a procedure that is intended to permanently remove genes that cause a particular disease'.[39] However, the birth of such a baby occurred much earlier than Cobb predicted: in 2018, the first genetically modified twins were born in China. Although the new method of 'gene improvement' raises immense controversies, it is also tied to huge hopes for effective treatment of genetic diseases. The question arises, Since this method offers the opportunity to eliminate the risk of all potential diseases from the DNA of the future child, should it be used at all? Or, as Grzegorz Lindenberg asks provocatively, should we maybe go even further and 'remove certain inconveniences, which are not serious diseases, but which make life harder for various reasons? Perhaps we should correct the genes so that the child is not born colour-blind? Or that, as an adult, he or she does not suffer from myopia or does not go bald prematurely? Another step that awaits us in relation to CRISPR leads from medical to aesthetic applications. Since we eliminate myopia in children, why not make boys taller, and give women bigger breasts, to increase their odds with the opposite sex? Why not improve musculature? Change the colour of eyes and hair? Boost intelligence? Give them more sensitivity, or quite the opposite – certain psychopathic traits (depending on what the parents believe would be more useful for the child)? In brief, let's design a custom child.'[40] While such visions are widely opposed, in 2018 the Nuffield Council on Bioethics in Great Britain decided that the alteration of DNA can be an option for parents who would like to influence the genetic makeup of their child. This is expected to apply not only to the removal of genetic defects but also to adding certain traits which, in the opinion of the parents, can facilitate the child's future success.[41] Thus, in the future, the CRISPR method may be used not only to treat genetic diseases and to prevent diseases at the embryo stage, but also to improve genes for aesthetic purposes. Finally, as the result of the method's use, human DNA could in the future be combined with the genes of animals, plants and even synthetic, laboratory-produced genes.[42] This could lead to the transformation of the current *Homo sapiens* species into some other species: the 'improved human' –

38 G. Lindenberg, Ludzkość poprawiona, *op. cit.*, p. 43ff.

39 M. Cobb, The Brave New World of Gene Editing, https://www.nybooks.com/articles/2017/07/13/brave-new-world-of-gene-editing/ (accessed 20.01.2020).

40 G. Lindenberg, Ludzkość poprawiona, *op. cit.*, p. 46.

41 S. Knapton, Designer Babies on Horizon as Ethics Council Gives Green Light to Genetically Edited Embryos https://www.telegraph.co.uk/science/2018/07/16/designer-babies-horizon-ethics-council-gives-green-light-genetically/ (accessed 20.01.2020).

42 G. Lindenberg, Ludzkość poprawiona, *op. cit.*, p. 48.

Homo sapiens+. Not only chimeras (with mixed genes from several persons) would be created, but also hybrids (human–animal, techno–human, techno–human–animal, etc.). This scenario can become true not only through genetics: information technologies and artificial intelligence would also certainly be helpful.

Speech synthesis and technological interfaces allow disabled persons to communicate with others already at this stage of biotechnological progress. Better functioning of the human body is also possible thanks to so-called smart drugs. These include nootropics (cognition-enhancing supplements) – consisting of various supplements and substances (including psychotropic ones). They are meant to enhance cognitive functions, such as memory, creativity, logical thinking, concentration, etc. These agents can also affect processes related to the nervous system, e.g. by increasing motivation and the will to live, delaying mental fatigue or improving mood. Thus, not only human organs but also the senses, memory and even such abilities as creativity or reasoning skills can be improved with the products of modern technologies. These technologies are the foundation of the new era whose advent is imminent and which is referred to as the 'computer-processing age' (or the 'age of cognitive systems' or the 'age of turbo-experience'). These technological 'boosters', equivalent to pills, capsules or syrups, can dramatically alter sensory experiences and perception of reality. The new generation of machines will not only think for humans, but also sensitize them, heighten their senses and even replace them. Machines will enable the making of better decisions. They will allow the removal of barriers that limit people, including barriers resulting from disability.

These predictions give hope for solving many problems related to existing human disabilities and for improving the condition of 'able-bodied' people. At the same time, it is not possible to disregard arguments that actions undertaken to create a perfect human are similar to 'playing God'. They represent a 'downward spiral', and their effects may be unimaginable from the perspective of individual rights, subjectivity, dignity, integrity, individuality, identity, freedom, equality, etc.[43] Above all, it is necessary to take into account the fears that in the future, people who are not genetically improved, or who are not fitted with computer parts, could become members of a sub-species with a status similar to the one currently accorded to animals.[44] Therefore it is extremely important to set ethical and legal boundaries for the application of technology.[45]

43 B. Chyrowicz, Bioetyka i ryzyko. Argument 'równi pochyłej' w dyskusji wokół osiągnięć współczesnej genetyki, Lublin 2002, p. 161ff.

44 M. Nowacka, Transumanistyczny sens prawa dziecka do otwartej przyszłości, (in:) P. Duchliński and G. Hołub (eds.), Ulepszanie moralne człowieka, *op. cit*., p. 115.

45 K. Trzęsicki, Medyczna etyka informatyczna: Przedmiot i główne problemy, „Archeus. Studia z bioetyki i antropologii filozoficznej" 2006, vol. 7, p. 66.

Conclusions

Modern technologies are able to limit, and even to eliminate – to a certain extent – problems tied to disability. They also allow the enhancement of the physical and mental capabilities of healthy persons. However, due to numerous ethical controversies, it is crucial to establish legal frameworks for actions that are made possible by biotechnological progress in medicine. These regulations should take into account the culturally defined standards of 'normality', which are difficult to define unambiguously. Undoubtedly, the fluidity of the criteria and the evolution of extra-legal considerations must be taken into account: 'We have long ago agreed to the improvement of our health condition through solutions such as spectacles for those with poor eyesight or the technical correction of the malfunctioning of the various organs. To what interventions would we agree in the subsequent phase of our civilization's development?'[46] It is difficult to provide a clear-cut answer. The supervision of biotechnological opportunities undoubtedly requires, in the first place, that boundaries be drawn, i.e. a distinction made between 'therapeutic' and 'improvement' activities.

Taking into account the dramatically limited access to treatment in Poland, it is hard to ruminate on the directions for the development and implementation of modern technologies in medicine.[47] Nevertheless, it appears that even despite enormous societal backwardness, the Polish philosophical and theoretical–legal discourse should consider the tendencies that dominate bioethics in developed countries. Bioethical reflection undoubtedly supports the holistic understanding of the concept of disability and its related problems. It helps resolve the emerging moral dilemmas and may constitute grounds for future legal regulations in this area.[48]

REFERENCES

Bączyk-Rozwadowska K., Prokreacja medycznie wspomagana. Studium z dziedziny prawa, Toruń 2018.

Bauman Z., Liquid Modernity, Cambridge 2000.

Chyrowicz B., Bioetyka i ryzyko. Argument 'równi pochyłej' w dyskusji wokół osiągnięć współczesnej genetyki, Lublin 2002.

Chyrowicz B., Spór o poprawianie natury ludzkiej, Lublin 2004.

Domaradzki J., Janusowe oblicze reprogenetyki, „Nowiny Lekarskie" 2009, no. 1, vol. 78.

46 M. Wojewoda, Jakość życia jako problem filozoficzny, „Folia Philosophica" 2018, no. 40, p. 109.

47 C. Szczylik, Jesteśmy onkologicznym bantustanem: To kompromitacja i cywilizacyjna porażka https://www.newsweek.pl/wiedza/nauka/onkologia-cezary-szczylik-chorowanie-na-nowotwor-w-polsce-to-koszmar/th1zzk3 (accessed 30.01.2020).

48 A. Przyłuska-Fiszer, Niepełnosprawność i rehabilitacja w perspektywie bioetyki, (in:) J. Głodkowska (ed.), Personalistyczne ujęcie fenomenu niepełnosprawności, Warsaw 2015, p. 82.

Domaradzki J., O definicjach zdrowia i choroby, „Folia Medica Lodziensia" 2013, no. 40.

Fry H., Jak być człowiekiem w epoce maszyn, Krakow 2018.

Galewicz W., Zdrowie jako prawo człowieka, „Diametros" 2014, no. 42.

Hołub G. (ed.), Ulepszanie człowieka. Fikcja czy rzeczywistość? Argumenty, krytyka, poszukiwanie płaszczyzny dialogu, Krakow 2018.

King D., Preimplantation Genetic Diagnosis and the 'New' Eugenics, "Journal of Medical Ethics" 1999, vol. 25.

Klichowski M., Narodziny cyborgizacji. Nowa eugenika, transhumanizm i zmierzch edukacji, Poznań 2014.

Kopania J., Projekt udoskonalenia człowieka w świetle relacyjnej koncepcji osoby, (in:) P. Duchliński and G. Hołub (eds.), Ulepszanie moralne człowieka. Perspektywa filozoficzna, Krakow 2019.

Leźnicki M. and Lewandowska A., Biomedykalizacja a genetyczne udoskonalanie człowieka w kontekście analiz bioetycznych, „Acta Universitatis Lodziensis" 2013, no. 45.

Lindenberg G., Ludzkość poprawiona. Jak najbliższe lata zmienią świat, w którym żyjemy, Krakow 2018.

Nawrot O., O zakresie dopuszczalności ingerencji wobec ludzkiego genomu, (in:) A. Białek and M. Wróblewski (eds.), Prawa człowieka a wyzwania bioetyczne związane z nowymi technologiami, Warsaw 2018.

Nowacka M., Transumanistyczny sens prawa dziecka do otwartej przyszłości (in:) P. Duchliński and G. Hołub (eds.), Ulepszanie moralne moralne człowieka. Perspektywa filozoficzna, Krakow 2019.

Plotz D., Fabryka Geniuszów. Niezwykła historia banku spermy noblistów, Warsaw 2007.

Przyłuska-Fiszer A., Niepełnosprawność i rehabilitacja w perspektywie bioetyki, (in:) J. Głodkowska (ed.), Personalistyczne ujęcie fenomenu niepełnosprawności, Warsaw 2015.

Savulescu J. and Bostrom N. (eds.), Human Enhancement, Oxford 2009.

Savulescu J., Deaf Lesbians, 'Designer Disability' and the Future of Medicine, "British Medical Journal" 2002, vol. 325.

Soniewicka M., Czemu ulepszanie genetyczne budzi sprzeciw?, „Filozofuj! Nowy człowiek?" 2017, vol. 6, no 18.

Soniewicka M., Selekcja genetyczna w prokreacji medycznie wspomaganej. Etyczne i prawne kryteria, Warsaw 2018.

Szymański K., Czy od transhumanizmu można uciec?, „Filozofuj! Nowy człowiek?" 2017, vol. 6 no. 18.

Trzęsicki K., Medyczna etyka informatyczna. Przedmiot i główne problemy, „Archeus. Studia z bioetyki i antropologii filozoficznej" 2006, vol. 7.

Wojewoda M., Jakość życia jako problem filozoficzny, „Folia Philosophica" 2018, no. 40.

Wolf M.W. and Kahn J.P., Using Preimplantation Genetic Diagnostoic to Create a Stem Cell Donor: Issues, Guidelines and Limits, "Journal of Law Medicine and Ethics" 2003, vol. 31.

Żuradzki T., Nowa liberalna eugenika: krytyczny przegląd argumentów przeciwko biomedycznemu poprawianiu ludzkiej kondycji fizycznej lub umysłowej, „Diametros" 2014, no. 42.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.06

Received: 10.03.2021
Accepted: 30.06.2021

Adam Wiśniewski
University of Gdańsk, Poland
adam.wisniewski@prawo.ug.edu.pl
ORCID ID: https://orcid.org/0000–0002-4921–0215

The European Court of Human Rights and Internet-Related Cases

Abstract: The Internet-related cases coming to the European Court of Human Rights provide a good illustration of the challenges posed to the protection of human rights as based on the European Convention of Human Rights drafted in 1950. Considering that the Convention is a 70-year-old instrument, the Strasbourg Court has to deal with these cases using the body of principles and interpretation methods and techniques that has been developed so far, and in particular the 'living instrument' doctrine. In this study I propose to explore some main threads in the Court's jurisprudence on Internet-related cases, outlining the specific nature of Internet-related cases, discussing the problem of rights connected with the Internet as well as the impact of the Internet on such classical rights as freedom of expression and the right to privacy. I conclude that the Internet-related case law of the Convention is in a process of constant development. The Strasbourg Court has demonstrated that it is capable of dealing with Internet-related cases based on general Convention norms and using its well-developed interpretation techniques. The striking feature of Strasbourg's case law is the ECtHR's recognition of the considerable importance of the Internet as regards the exercise of freedom of expression, and in particular freedom to seek and access information. Although the ECtHR regards the Internet as a communication medium, however, it recognises its specific features which affect the performance of rights protected by the Convention as well as dangers it poses for the protection of human rights under the European Convention of Human Rights.
Keywords: human rights, Internet, the European Convention of Human Rights, the European Court of Human Rights

Introduction

Technological advancements undoubtedly have considerable implications for human rights. It is true to say that these implications can be beneficial from the

point of view of securing the protection of human rights. Nevertheless, technological progress, resulting in advancements such as developments in artificial intelligence, automation and robotics, raises serious questions about the potentially adverse impact on human rights. The development of the Internet during the last thirty years has certainly been one of the most important technological inventions; its emergence has significantly affected a number of aspects of everyday life, including, in particular, communication, learning, working, shopping, etc. It has also enabled new forms of social interaction, activities and social associations. However, it is no wonder that the use of the Internet creates a number of problems from the point of view of the protection of human rights.

International human rights treaties adopted after the Second World War were drafted at a time when the Internet was not known in societies. In this study, I propose to analyse some aspects of the impact of the Internet on human rights, taking as an example the European Convention of Human Rights ('the Convention' or 'ECHR'), signed in Rome on 4 November 1950. It is undoubtedly the most important instrument among conventions adopted within the Council of Europe and the most important regional instrument in the field of human rights in Europe. The Convention, as well as the case law of the European Court of Human Rights ('the Court' or 'the ECtHR') acting on its basis, provides standards for the protection of these rights for the 47 Member States of the Council of Europe.

The Convention is a relatively old international instrument, and when it was adopted more than 70 years ago, the aforementioned technological advancements of modernity could not have been taken into account by its drafters. It should be noted that the ECHR contains general norms and obligations providing only the framework which states 'have the duty to fill in with their own content'.[1] Therefore, the challenges posed to the protection of human rights in the ECHR by technological advancements have to be dealt with by the European Court of Human Rights, whose task, according to Article 19 of the Convention, is to ensure the observance of the engagements undertaken by the High Contracting Parties in the Convention and the Protocols. The Strasbourg Court, whose jurisdiction extends, according to Article 32 Section 2 of the ECHR, to all matters concerning the interpretation and application of the Convention and the Protocols, has developed a body of principles, interpretation methods and techniques to deal with this task, and one of the most important of those methods is the 'living instrument' doctrine, allowing the Court to interpret the Convention norms in the light of present-day conditions.[2]

1 C. Mik, Charakter, struktura i zakres zobowiązań z Europejskiej Konwencji Praw Człowieka, „Państwo i Prawo" 1992, no. 4, p. 5.

2 The Court has observed on many occasions that the Convention is to be seen 'a living instrument which must be interpreted in the light of present-day conditions'; Judgement of the ECtHR of 25 April 1978 on the case of application no. 5856/72, § 31. See also S. Flogartis, T. Zwart and J. Fraser,

The aim of this article is to explore some of the main threads in the Court's jurisprudence concerning Internet-related cases with the assumption that its case law reflects the most important challenges for human rights posed by the Internet. This study is by no means exhaustive; instead it focuses on some selected issues connected with Internet-related cases. After outlining the specific nature of Internet-related cases, I will discuss the problem of rights connected with the Internet as well as the impact of the Internet on such classical rights as freedom of expression and the right to privacy, with the aim of arriving at some more general observations and conclusions concerning the tendencies in the Internet-related Strasbourg case law.

1. The Specific Nature of Internet-Related Cases

Internet-related cases involve quite complex jurisdictional issues. According to Article 1 of the ECHR, the state parties to the Convention are obliged to 'secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention'. The state parties thus may be held responsible for any violation of the protected rights and freedoms of anyone within their 'jurisdiction' – or competence – at the time of the violation.[3] The exercise of jurisdiction is thus a necessary condition for holding a contracting state responsible for acts or omissions imputable to it which resulted in an allegation of the infringement of Convention rights and freedoms.[4]

The notion of 'jurisdiction' within the meaning of Article 1 of the Convention should be understood, in the light of international law, as primarily territorial, so it is presumed to be exercised usually throughout the state's territory.[5] In certain cases, the ECtHR extends the territorial jurisdiction to other areas which, at the time of the alleged violation, were, for example, under the 'overall control' of the state concerned.[6] However, the issue of whether exceptional circumstances exist which require and justify a finding by the Court that the state was exercising jurisdiction extra-territorially must be determined every time with reference to particular facts, for example full and exclusive control over a prison or a ship.[7]

The European Court of Human Rights and its Discontents. Turning Criticism into Strength, Cheltenham/Northampton 2013, pp. 198–199.

3 Judgement of the ECtHR of 8 April 2004 on the case of Assanidze v. Georgia, application no. 71503/01, § 137.

4 Judgement of the ECtHR of 8 July 2004 on the case of Ilaşcu and Others v. Moldova and Russia, application no. 48787/99, § 311.

5 Assanidze v. Georgia, *op. cit.*, § 139.

6 Judgement of the ECtHR of 23 March 1995 on the case of Loizidou v. Turkey, application no. 15318/89.

7 Judgement of the ECtHR of 7 July 2011 on the case of Al-Skeini and Others v. the United Kingdom, application no. 55721/07, § 132. See also E. Karska and K. Karski, Introduction: Extraterritorial Scope of Human Rights, "International Community Law Review" 2015, vol. 17, no. 4–5, pp. 395–401.

In a number of cases, the Court recognised the exercise by a contracting state of its 'jurisdiction' outside its territory within the meaning of Article 1 of the Convention. The crucial condition in these cases is whether the state party to the Convention exercised effective power and control outside its national territory. In its first judgement in Loizidou v. Turkey, the Court ruled that, bearing in mind the object and purpose of the Convention, the responsibility of a contracting party may also arise when as a consequence of military action – whether lawful or unlawful – it exercises effective control of an area outside its national territory.[8]

The characteristic feature of Internet-related cases is a cross-border element. In the case of communication via the Internet, the data are usually transmitted via servers located in various territorial jurisdictions. This sometimes results in considerable difficulties when it comes to establishing which state has jurisdiction in a given case.

Considering this specific condition, it is surprising, firstly, that there have so far been relatively few Internet-related cases concerning jurisdictional issues in Strasbourg.[9] Secondly, it is noteworthy that the Court appears generally in favour of the assertion of the state party of its own jurisdiction. An illustration of this can be seen in the case of Perrin v. the United Kingdom, in which the applicant, a French national living in the United Kingdom, was charged and subsequently convicted in the UK by the Crown Court for publishing obscene content on three different web pages. Contesting his convictions, the applicant raised, among other things, that publication of the web pages had taken place outside UK jurisdiction. He argued that English courts should only be able to convict when the major steps towards publication took place within their jurisdiction. Addressing this jurisdictional point, the Court of Appeal noted that 'the applicant's suggestion, that conviction should only be possible where major steps had been taken towards publication in a place over which the court had jurisdiction, would undermine the aim that the law was intended to protect by encouraging publishers to take the steps towards publication in countries where they were unlikely to be prosecuted'. This line of reasoning was accepted by the ECtHR who declared the application inadmissible.[10]

The specific nature of the Internet-related cases stems also from certain features of the Internet in the context of human rights. In its case law involving alleged violations of rights in connection with the Internet, the Strasbourg Court has made some important observations concerning features of the Internet in the

8 Loizidou v. Turkey, *op. cit.*, § 62.

9 See Internet: Case-law of the European Court of Human Rights, Council of Europe, 2011, updated June 2015, p. 6, https://www.echr.coe.int/documents/research_report_internet_eng.pdf (accessed 25.04.2021).

10 Decision of the ECtHR of 18 October 2005 as to the admissibility of the case of Perrin v. the United Kingdom, application no. 5446/03, p. 3.

context of rights protected under the ECHR. The Internet has been evaluated from the perspective of its beneficial impact on the exercise of some protected rights, in particular the freedom to receive information, as well as some of its potentially adverse effects on the exercise of some rights, such as rights to privacy. First of all, the ECtHR has emphasised the importance of Internet sites in the exercise of freedom of expression, in particular as regards the facilitation of receiving information. According to the Court, 'the Internet has now become one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas'.[11] In the case of Times Newspapers Ltd v. the United Kingdom, the Court emphasised the significance of the Internet, especially in the context of the right to receive information protected under Article 10, by saying that 'in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10.'[12] Moreover, the Strasbourg Court has stressed 'the substantial contribution made by Internet archives to preserving and making available news and information. Such archives constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free.'[13]

The Strasbourg Court considers Internet sites as 'an information and communication tool'.[14] However, it points out the difference between the Internet and printed media. According to the ECHR, this difference is particularly visible as regards the capacity to store and transmit information. It is also visible as regards regulations and control. As the ECtHR observed, the Internet, 'as the electronic network which serves billions of users worldwide, is not and potentially will never be subject to the same regulations and control as printed media'.[15] Furthermore, 'the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press', the reason being, in particular, the important role of search engines.[16] The specificity of the Internet also lies in 'the

11 Judgement of the ECtHR of 1 December 2015 on the case of Cengiz and Others v. Turkey, application nos. 48226/10 and 14027/11, § 49.

12 Judgement of the ECtHR of 10 March 2009 on the case of Times Newspapers Ltd nos. 1 and 2 v. the United Kingdom, application nos. 3002/03 and 23676/03, § 27.

13 *Ibidem*, §§ 27 and 45.

14 Judgement of the ECtHR of 5 May 2011 on the case of Editorial Board of PravoyeDelo and Shtekel v. Ukraine, application no. 33014/05, § 63.

15 *Ibidem*.

16 Judgement of the ECtHR of 28 June 2018 on the case of M.L. and W.W. v. Germany, application nos. 60798/10 and 65599/10, § 91.

ease, scope and speed of the dissemination of information on the Internet, and the persistence of the information once disclosed'.[17] This, as the Court observed, 'may considerably aggravate the effects of unlawful speech on the Internet compared to traditional media'.[18]

One of the consequences of these particular features of the Internet pointed out by the Court is that 'the policies governing reproduction of material from the printed media and the Internet may differ. The latter undeniably have to be adjusted according to the technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned.'[19]

The Court is not blind as regards the sometimes serious threats to the protection of Convention rights connected with the Internet, noticing, inter alia, that 'the rapid development of telecommunications technologies in recent decades has led to the emergence of new types of crime and has also enabled the commission of traditional crimes by means of new technologies'.[20] It is, however, primarily up to states to take proper measures and introduce adequate safeguards. As the Court put it in the case of K.U. v. Finland concerning child sexual abuse on the Internet, 'it was well-known that the Internet, precisely because of its anonymous character, could be used for criminal purposes… Also, the widespread problem of child sexual abuse had become well known over the preceding decade. Therefore, it cannot be said that the respondent Government did not have the opportunity to put in place a system to protect child victims from being exposed as targets for pedophiliac approaches via the Internet.'[21]

The recognition by the Court of such threats and dangers is reflected, among others, in its case law concerning the liability of host providers, administrators, etc. for posting insulting, vulgar comments, etc., which will be discussed in the point concerning 'Freedom of Expression and the Internet'. This position of the Court regarding the role of Internet, outlined above, has apparently had considerable impact on the ECtHR's approach towards the two rights usually mentioned in connection with the Internet, namely regarding the right of access to the Internet and the right to be forgotten.

2. Rights Connected with the Internet

2.1 Right of Access to the Internet

The importance of the Internet, especially from the point of view of enhancing freedom of expression, begs the question of access to the Internet and in particular

17 Judgement of the ECtHR of 16 June 2015 on the case of Delfi AS v. Estonia, application no. 64569/09, § 147.

18 *Ibidem*.

19 Editorial Board v. Ukraine, *op. cit.*, § 67.

20 Judgement of the ECtHR of 2 December 2008 on the case of K.U. v. Finland, application no. 2872/02, § 22.

21 *Ibidem*, § 48.

whether there exists some right of access to the Internet. It is noteworthy that access to the Internet can be understood either as access to content or access to the technical infrastructure required to access the Internet.

The matter of access to the Internet has gained some recognition at the UN level. For example, the report of the Special Rapporteur to the UN General Assembly stated: 'Given that the Internet has become an indispensable tool for realising a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States. Each State should thus develop a concrete and effective policy, in consultation with individuals from all sections of society, including the private sector and relevant Government ministries, to make the Internet widely available, accessible and affordable to all segments of population.'[22] It is noteworthy that the report confirms two dimensions of Internet access, that is, access to content and access to the physical and technical infrastructure required to access the Internet.[23] Referring to this report, the Human Rights Council adopted the resolution on the 'Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development' on 16 July 2012, in which, among other things, it called upon all states 'to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries'.[24] Also, in the resolution of 2016, the Council condemned 'unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law and calls on all States to refrain from and cease such measures'.[25]

A similar approach was adopted by other international organisations. For example, in its report of 2011, the Organization for Security and Co-operation in Europe emphasised that 'Everyone should have a right to participate in the information society and states have a responsibility to ensure citizens' access to the Internet is guaranteed.'[26] In EU law, Internet access is not as yet included among the fundamental rights and principles, and according to EU policy documents,

22 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, GE.11–13201, 16 May 2011, https://www2.ohchr.org/english/bodies/hrcouncil/docs/ 17session/A.HRC.17.27_en.pdf (accessed 26.04.2021).

23 *Ibidem*, p. 1.

24 Human Rights Council: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement (accessed 23.06.2021).

25 Human Rights Council: The promotion, protection and enjoyment of human rights on the Internet, 27 June 2016, https://www.article19.org/data/files/Internet_Statement_Adopted.pdf (accessed 23.06.2021).

26 Organization for Security and Co-operation in Europe, 'Freedom of Expression on the Internet: A study of legal provisions and practices related to freedom of expression, the free flow of

Internet access is regarded a tool which can contribute to improving the functioning of the internal market by generating economic wealth and can also provide some social benefits to citizens.[27] Under the Directive 2002/22 / EC on universal service and users' rights relating to electronic communications networks and services as amended in 2009 by Directive 2009/136 / EC, recital 5612, the EU Member States are required to adopt domestic measures implementing the objectives of the Directive, such as providing access to a broadband connection at fixed points. The Directive also establishes a minimum quality standard for Internet access.[28]

In the context of these developments, the outstanding document is certainly Resolution 1987 on 'The right to Internet access', issued by the Parliamentary Assembly of the Council of Europe in 2014, in which the Assembly recommended that the Council of Europe's Member States ensure the right to Internet access on the basis of principles mentioned in this resolution.[29] These principles include, among others, the recognition that the right to Internet access is an essential requirement for exercising rights under the European Convention on Human Rights, that the right to Internet access includes the right to access, receive and impart information and ideas through the Internet without interference from public authorities, and that Internet access is also essential for the exercise of other human rights, such as the right to freedom of assembly and the right to private and family life, therefore Member States should recognise the fundamental right to Internet access in law and in practice.[30]

Based on these developments, some authors have expressed the view that 'nowadays it is possible to say that access to the Internet is gradually becoming an independent human right'.[31] At the national level, however, only a few countries have decided to introduce the right of access to the Internet, usually in some limited form. For example, Estonia introduced the right of access to the public Internet through an

information and media pluralism on the Internet in OSCE participating States', 15 December 2011, https://www.osce.org/files/f/ documents/e/f/80723.pdf (accessed 23.06.2021), p. 38.

27 L. Jasmontaite and P. de Hert, Access to the Internet in the EU: A Policy Priority, a Fundamental, a Human Right or a Concern for eGovernment? 'Brussels Privacy Hub Working Paper' February 2020, vol. 6, no. 19, p. 5, https://www.researchgate.net/publication/339860840_Access_to_the_Internet_in_the_EU_a_policy_priority_a_fundamental_a_human_right_or_a_concern_for_eGovernment(accessed 23.06.2021).

28 See *ibidem*, pp. 3–21.

29 Resolution 1987 (2014), 'The right to Internet access', https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20870&lang=en (accessed 24.06.2021).

30 *Ibidem*, paragraphs 5.1., 5.2. and 5.4.

31 See, for example, M. Zieliński, Dostęp do Internetu jako prawo człowieka? W sprawie potrzeby nowej wolności w konstytucji Rzeczypospolitej Polskiej, 'Przegląd Sejmowy' 2013, no. 4, pp. 21–22; M.L. Best, Can the Internet Be a Human Right? (in:) S. Hick, E.F. Halpin and E. Hoskins (eds.), Human Rights and the Internet, New York 2000, p. 24.

Internet link, and in Finland the relevant provisions of law provide for the obligation of telecommunication operators to ensure a proper Internet link.[32]

Against this background it may be rather surprising that the Strasbourg Court appears to be slow and perhaps somewhat reluctant to recognise the general right of access to the Internet under Article 10 of the ECHR, although its rulings in this area depend to a large extent on the specific circumstances of the case. For example, in the case of Kalda v. Estonia, the Court found that there is no right of access to the Internet for prisoners, following from Article 10 of the Convention. The case concerned an applicant, a prisoner in Estonia, who complained that the authorities' refusal to grant him access to certain websites violated his right to receive information 'without interference by public authority', in breach of Article 10 of the Convention. The Court, observed, however, that: 'imprisonment inevitably involves a number of restrictions on prisoners' communications with the outside world, including their ability to receive information', and according to the ECtHR, 'Article 10 cannot be interpreted as imposing a general obligation to provide access to the Internet, or to specific Internet sites, for prisoners. However, it finds that in the circumstances of the case, since access to certain sites containing legal information is granted under Estonian law, the restriction of access to other sites that also contain legal information constitutes an interference with the right to receive information.'[33] The finding of the violation of Article 10 of the Convention in this case was the result of finding that the interference with the applicant's right to receive information, in the specific circumstances of the present case, cannot be regarded as having been necessary in a democratic society.[34]

An interesting approach to access to the Internet in prison was adopted by the Court in the case of Mehmet Reşit Arslan and Orhan Bingöl v. Turkey, in which the applicants, serving sentences of life imprisonment as a result of their convictions for membership of an illegal armed organisation, complained that they were being prevented from using a computer and accessing the Internet, i.e. resources essential in order for them to continue their higher education and improve their general knowledge. Interestingly, the Court held that there had been a violation of Article 2 (the right to education) of Protocol No. 1 to the Convention in respect of both applicants, finding that domestic courts had failed to strike a fair balance between their right to education on the one hand and the imperatives of public order on the other. Moreover, the Court observed, in particular, that the importance of education in prison had been recognised by the Committee of Ministers of the Council of

32 See J. Rzucidło, Prawo dostępu do internetu jako podstawowe prawo człowieka: Część I, „Kwartalnik Naukowy Prawo Mediów Elektronicznych" 2010, no. 2, p. 38.

33 Judgement of the ECtHR of 19 January 2016 on the case of Kalda v. Estonia, application no. 17429/10, § 45.

34 *Ibidem*, § 54.

Europe in its recommendations on education in prison and in its European Prison Rules.[35]

In a number of cases, mostly against Turkey and Russia, the Court had to deal with the blocking of access to the Internet by domestic authorities. The blocking was found acceptable if it was made on grounds such as the protection of copyright. In the case of Akdeniz v. Turkey, the blocking of access to two websites was effected on the grounds that they streamed music without respecting copyright legislation. The application in this case was lodged by the applicant who was a user of the websites in question. The ECtHR declared the application inadmissible on the grounds that the applicant could not claim to be a 'victim' in the sense of Article 34 of the Convention. Although the rights of Internet users were declared to be of paramount importance, nevertheless the Court observed that the two music-streaming websites in question had been blocked because they operated in breach of copyright law. Moreover, the Court further observed that the applicant had at his disposal many means to access a range of musical works without thereby contravening the rules governing copyright.[36]

The Court is more likely to find a violation if the blocking of websites takes place due to other reasons than the protection of copyright. In the case of Ahmet Yıldırım v. Turkey, a Turkish court decided to block access to Google Sites hosting an Internet site whose owner was involved in criminal proceedings for insulting the memory of Atatürk. The applicant complained that he was deprived of access to his own Internet site because of this measure, which was ordered in the context of criminal proceedings without any connection to him or his site. The Court found a violation of Article 10 on the ground of the principle of proportionality, namely, that the decision to block all access to Google Sites was made 'without ascertaining whether a less far-reaching measure could have been taken to block access specifically to the offending website'.[37] Moreover, the effects of the measure in question had been arbitrary and the judicial review of the blocking of access had been insufficient to prevent abuses.[38]

In the case of Cengiz and Others v. Turkey, the applicants had been deprived of all access to YouTube as a result of a court order, on the grounds that a post on YouTube had infringed the country's criminal law which prohibited insulting the memory of Mustafa Kemal Atatürk. The Court found that there was a violation of Article 10 of the Convention. As in the case of Ahmet Yıldırım, according to the Court the authorities should have taken into consideration the fact that the measure

35 Judgement of the ECtHR of 7 October 2019 on the case of Mehmet Reşit Arslan and Orhan Bingöl v. Turkey, application nos. 47121/06, 13988/07 and 34750/07, *§ 69–72*.

36 Decision of the ECtHR of 11 March 2014 as to the admissibility of the case of Akdeniz v. Turkey, application no. 20877/10.

37 Judgement of the ECtHR of 18 December 2012 of the case of Ahmet Yıldırım v. Turkey, application no. 3111/10, § 64.

38 *Ibidem*.

in question was bound to substantially restrict the rights of Internet users and to have a significant collateral effect by rendering large quantities of information inaccessible. Moreover, as a result of the ordered measure, the applicants had no access to YouTube for a lengthy period.[39]

In cases where blocking access to a website was a result of a measure imposed before a final ruling by a court, such blocking was considered as a prior restraint. According to the ECHR, prior restraints are not necessarily incompatible with the Convention as a matter of principle.[40] Nevertheless, the Court pointed out that a legal framework is required, ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse of power. What is important is that such a framework should establish 'precise and specific rules regarding the application of preventive restrictions on freedom of expression'.[41] Moreover, within such a framework there should be the possibility of judicial review of a questioned measure, such as the one blocking access to a particular website. Such a review should be based on a weighing-up of the competing interests at stake and be designed to strike a balance between them.[42]

Likewise, in the case of Kablis v. Russia, the applicant's access to three blog entries had been restricted on the order of the Prosecutor General's office because they had been found to contain calls to participate in public events held in breach of established procedure. As the Court observed, the aim of the public event in question was to express an opinion on an important issue of public interest, namely the recent arrest of regional government officials. The Court reminded that under its case law, 'expression on matters of public interest is entitled to strong protection' and that 'very strong reasons are required for justifying such restrictions'.[43] Nevertheless, the domestic authorities failed to advance any reasons for blocking access to the two above-mentioned posts and did not explain why they had been included in the blocking measure, even though they did not contain any calls for participation in a public event held in breach of established procedure. Finding a violation of Article 10 in this case, the Court also pointed out that the domestic law lacked the necessary guarantees against abuse required by the Court's case law for prior restraint measures.[44]

The important lesson following from the above judgements is that the blocking of Internet sites, even if it amounts to prior restraint, is not as such incompatible with the Convention. However, it needs to meet certain requirements laid down in

39 Cengiz and Others v. Turkey, *op. cit.*, § 57.
40 Yıldırım v. Turkey, *op. cit.*, § 47.
41 *Ibidem*, § 67.
42 *Ibidem*.
43 Judgement of the ECtHR of 30 April 2019 on the case of Kablis v. Russia, application nos. 48310/16 and 59663/17, § 101.
44 *Ibidem*, § 106.

Strasbourg case law. In particular, the proper legal framework should be established, providing precise and specific rules and allowing domestic courts to adequately balance competing interests. Moreover, strong reasons need to be provided in cases where restrictions are imposed on public debate and on political speech. The necessary test involving proportionality plays an important role in deciding such cases by the Strasbourg Court. As one author observed, in a number of cases, states failed to comply with the requirements of this test and the principle of proportionality connected with it, especially because there were less intrusive methods available.[45] It follows from Strasbourg case law that restrictions on Internet access are considered to be a drastic limitation of freedom of expression and are treated as the measure of last resort, which has to be supported by very convincing reasons.

2.2. The Right to Be Forgotten

One of the rights which is nowadays commonly associated with the Internet is the 'right to be forgotten' which was, as is sometimes presented, introduced by the Court of Justice of the European Union in its judgement of 13 May 2014 on the case C 131/12, Google Spain sl v. AEPD (the DPA) & Mario Costeja González. The case originated in the complaint brought in March 2010 by a Spanish national, Costeja González, before the country's data protection agency (AEPD) against La Vanguardia newspaper, Google Spain, and Google Inc. In his complaint, Mr González demanded the removal or alteration of the record of legal action taken against him concerning the auction of his property in 1998. The information should be removed, he argued, because the proceedings were concluded years earlier and there was no outstanding claim against Mr González. The fact that the information continued to feature prominently had been damaging his reputation. The complaint against Google was upheld on the ground that search engines are also subject to data protection laws and must take necessary steps to protect personal information. As the result of Google Inc.'s and Google Spain's appeals against the decision of the AEPD, the National High Court of Spain decided to stay the proceedings and request the EU Court of Justice give a preliminary ruling.

The Court of Justice found Mr González had the right to request the erasure of his personal data from Google and, consequently, Google had the obligation to erase them.[46] In its reasoning, the CJ considered that although search engines have the right to process personal data when this is necessary in order for the legitimate interest of the data holder or the interests of third parties, this right is not, however,

45 G. Gosztonyi, European Court of Human Rights: Internet Access as a Means of Receiving and Imparting Information and Ideas, 'International Comparative Jurisprudence' 2020, vol. 6, no. 2, p. 139, https://ojs.mruni.eu/ojs/international-comparative-jurisprudence/article/view/6292 (accessed 21.04.2021).

46 Judgement of the Court of Justice of 13 May 2014 on the case of Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C 131/12, p. 21.

absolute and may be limited when it collides with the interests or the fundamental rights of the data subject, in particular the right to privacy.[47]

The right to be forgotten was confirmed in Article 17 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which repealed Directive 95/46 / EC (the General Data Protection Regulation) entitled 'Right to erasure ('right to be forgotten')' which provides that 'The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where… the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.'

However, in its case law the ECtHR appeared to be reluctant to recognise the right to be forgotten on the Internet.[48] One of the examples of this position can be seen in the judgement on the case of M.L. and W.W. v. Germany, in which the applicants alleged a violation of Article 8 of the ECHR on account of the decision of the Federal Court of Justice not to prohibit various media outlets from making old reports – or transcripts thereof – concerning the applicants' criminal trial available on the Internet. The applicants were sentenced to life imprisonment for the 1991 murder of W.S, a very popular actor. After being released from prison in 2008, they brought actions against a German radio station and a weekly magazine, asking that articles and radio interviews relating to the murder case be removed from their website archives.

In the substantiation of its judgement, the Strasbourg Court acknowledged, among other things, that the concept of 'private life' refers to 'personal information which individuals can legitimately expect should not be published without their consent'.[49] The ECtHR analysed in some depth, among others, the judgement of the Court of Justice of the European Union of 13 May 2014 (Google Spain and Google) as well as the relevant EU law on this. However, the Strasbourg Court finally found that there had been no violation of the right to privacy of the applicants protected under Article 8 of the Convention. However, the Court observed that in order for Article 8 to become applicable, 'an attack on a person's reputation must attain a certain level of seriousness and in a manner causing prejudice to personal enjoyment of the right to

47 As some authors point out, this judgement is regarded as 'a point of reference in the protection of personal data in the European [sic], but also the international level'. See K. Kakavoulis, The case Google Spain v. AEPD and Mario Costeja Gonzalez of the Court of Justice of the European Union: A Brief Critical Analysis, https://www.homodigitalis.gr/en/posts/2900 (accessed 24.04.2021).

48 V. Szeghalmi, Difficulties Regarding the Right to Be Forgotten in the Case Law of the Strasbourg Court, "Athens Journal of Law" 2018, vol. 4, no. 3, p. 270.

49 Judgement of the ECtHR of 28 June 2018 on the case of M.L. and W.W. v. Germany, application nos. 60798/10 and 65599/10, § 86.

respect for private life. Moreover, Article 8 cannot be relied on in order to complain of a loss of reputation which is the foreseeable consequence of one's own actions such as, for example, the commission of a criminal offence.'[50]

The case was decided by using the balancing method combined with the margin of appreciation doctrine. Thus the ECtHR balanced the right to privacy protected under Article 8 against freedom of expression and freedom to access information under Article 10 of the European Convention, holding, however, that national authorities enjoy the margin of appreciation in weighing up diverging interests in this case.[51] Nevertheless, behind the veil of the margin of appreciation doctrine lies the appreciation by the Court, declared elsewhere in this judgement, of the importance of the Internet, especially 'as a source for education and historical research, particularly as they are readily accessible to the public and are generally free'.[52] The ECtHR went further, emphasising 'the establishment of digital archives, which contribute significantly to enhancing the public's access to information and its dissemination',[53] and, most importantly, said that according to its case law, 'the legitimate interest of the public in access to the public Internet archives of the press is protected under Article 10 of the Convention, and particularly strong reasons must be provided for any measure limiting access to information which the public has the right to receive'.[54] Thus, the Court clearly took a position in favour of the presumption of uninhibited access by the public to Internet archives. The margin of appreciation concept was in fact used as an indication of acceptance by the ECtHR of the position taken in this case by German courts in particular that there is a very high public interest in being able to access information about important past events such as the murder case at issue. It is thus no wonder that some authors correctly point out that the current case law of the Strasbourg Court appears to indicate that the ECtHR is more in favour of a right to remember, appearing to be rather reluctant to recognise the right to be forgotten in the online sphere.[55] The right to remember for the Court amounts to free access by the public to information that can be found on the Internet, whereas the right to be forgotten appears to be limiting access to information which the public has the right to receive.

A position in favour of the right to be forgotten was taken by the Court in the case of Hurbain v. Belgium, in which the applicant complained that he had been ordered to anonymise the archived version of an article on his newspaper's website. The article in question was published in the newspaper *Le Soir* and reported on a car

50 *Ibidem*, § 88.
51 *Ibidem*, § 116.
52 *Ibidem*, § 90.
53 *Ibidem*, § 102.
54 *Ibidem*.
55 V. Szeghalmi, Difficulties, *op. cit.*, p. 270.

accident that had caused the deaths of two persons and injured three others. In this article, the full name of a driver who had been responsible for this road accident was mentioned. The driver, who had been convicted in 2000, had served his sentence and was rehabilitated in 2006, sued Mr Hurbain successfully in 2012 to obtain the anonymisation of the press article about him. In its judgement, the Court agreed with the domestic courts' findings that keeping the article online could cause indefinite and serious harm to the driver's reputation, creating a sort of 'virtual criminal record' despite the fact that the driver had already been rehabilitated after serving his sentence after a final conviction. Finding that the Belgian courts had weighed up the driver's right to respect for his private life on the one hand and Mr Hurbain's freedom of expression on the other, in accordance with the criteria laid down in the Court's case law, the Strasbourg Court held that there had therefore been no violation of Article 10 in the case.[56]

3. Freedom of Expression and the Internet

As was already mentioned, the Court has repeatedly stressed in its case law the importance of Internet sites for the exercise of freedom of expression. The Internet is correctly regarded as a means of communication, and freedom of expression on the Internet is protected under Article 10 of the Convention.[57] This protection extends regardless of the type of message or the purpose of its publication. Therefore, publications for commercial purposes are also covered. For example, the publication of photographs on an Internet site devoted to fashion which offered the public pictures of fashion shows either for sale or for consultation (the latter free of charge or for a fee) was considered as protected under Article 10 of the Convention.[58]

The Court applies the same principles concerning freedom of expression developed in its case law under Article 10 to freedom of expression on the Internet, confirming, among other things, that 'freedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment'. Subject to Paragraph 2 of Article 10, it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend,

56 Judgement of the ECtHR of 22 June 2021 on the case of Hurbain v. Belgium, application no. 57292/16 (in French), §§ 125–133.

57 Internet: Case-law, *op. cit.*, p. 17.

58 Judgement of the ECtHR of 10 January 2013 on the case of Ashby Donald and Others v. France, application no. 36769/08, § 34.

shock or disturb. Such are the demands of pluralism, tolerance and broadmindedness, without which there is no 'democratic society'.[59]

Therefore, the Court is willing to grant strong protection and allow a corresponding narrow margin of appreciation for domestic authorities in the case of political speech, and weaker protection and a wider scope of the margin of appreciation in the case of commercial speech.[60] The strong protection of political speech is closely connected with the role of the press as the '*public watchdog*' in a democratic society whose task is to control the government. Therefore the press is entitled to the wider limits of freedom of expression under Article 10 of the Convention as well.[61] The application of these principles by the Court to freedom of expression on the Internet leaves little room for concepts such as the right to be forgotten.

Moreover, certain categories of speech are excluded from the protection of Article 10 of the Convention, regardless of whether the speech is communicated on the Internet or through other media of communication. This refers in particular to hate speech which is insulting to particular individuals or groups or any other speech incompatible with the values of the Convention.[62] The Court is also very likely to reject an application in the case of offensive and injurious speech on the Internet that goes beyond merely satirical and defamatory expression.[63]

Despite the application by the Court of the same general principles developed in its case law concerning Article 10 of the ECHR to freedom of expression in Internet-related cases, there are still some specific issues in these cases which the Court has to deal with. An interesting comparative analysis of the impact of radio and television as contrasted with the Internet was carried out by the Court in the case of Animal Defenders International v. the United Kingdom concerning the statutory prohibition of paid political advertising on radio and television. The applicant argued that limiting the prohibition in question to radio and television was illogical, taking into account the comparative potency of newer media such as the Internet. The ECtHR disagreed, finding a distinction based on the particular influence of the broadcast media to be coherent, and said that 'the Court recognizes the immediate and powerful effect

59 See, for example, the Judgement of the ECtHR of 22 April 2013 on the case of Animal Defenders International v. the United Kingdom, application no. 48876/08, § 100.

60 See L. Garlicki (ed.), Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I, Komentarz do artykułów 1–18, Warsaw 2010, pp. 626–627; A. Wiśniewski, Koncepcja marginesu oceny w orzecznictwie Europejskiego Trybunału Praw Człowieka, Gdańsk 2008, pp. 214–215.

61 S.C. Prebensen, The Margin of Appreciation and Articles 9, 10 and 11 of the Convention, 'Human Rights Law Journal' 1998, vol. 19, no. 1, p. 14.

62 See, for example, the Judgement of the ECtHR of 4 December 2003 on the case of Gündüz v. Turkey, application no. 35071/97, § 41.

63 Judgement of the ECtHR of 11 March 2014 on the case of Bartnik v. Poland, application no. 53628/2010; see also Internet: Case-law, *op. cit.*, p. 20.

of the broadcast media, an impact reinforced by the continuing function of radio and television as familiar sources of entertainment in the intimacy of the home. In addition, the choices inherent in the use of the Internet and social media mean that the information emerging therefrom does not have the same synchronicity or impact as broadcasted information. Notwithstanding therefore the significant development of the Internet and social media in recent years, there is no evidence of a sufficiently serious shift in the respective influences of the new and of the broadcast media in the respondent State to undermine the need for special measures for the latter.'[64]

The Court also had to deal in its case law with the issue of the liability of the owner of an Internet news portal for defamatory comments posted in its commenting area. The applicant company complained that holding it liable for the comments posted by the readers of its Internet news portal infringed its freedom of expression. However, the ECtHR considered the insulting and threatening nature of the comments, as well as the fact that these comments were posted in reaction to an article published by the applicant company in its professionally managed news portal run on a commercial basis. Moreover, the Court found the measures taken by the applicant company to avoid damage being caused to other parties' reputations and to ensure a realistic possibility that the authors of the comments will be held liable to be insufficient. For example, the automatic word-based filter which was applied was relatively easy to circumvent, thus failing to prevent some insults or threats.[65] Taking into account a relatively moderate sanction imposed on the applicant company, the Court found no violation of Article 10, setting a standard, however, for effective prevention by media companies for insulting or defamatory posted comments. It is noteworthy that the Court omitted in its consideration the Directive on Electronic Commerce[66] (although it is mentioned in the judgement), which governs the liability regime of host providers. It is worth mentioning that under this regime, hosting providers are not liable for information they store if they do not have actual knowledge of its illegal nature or if they act expeditiously to remove or disable access to that information as soon as they become aware of it.

Some Internet-related cases concern the question of the liability of the media for making accessible various content from Internet sites. An interesting ECtHR judgement concerning the liability of media companies for content hyperlinked in their articles or reports published online was issued in the Magyar JetiZrt v. Hungary case. The Strasbourg Court, finding a violation of Article 10 of the Convention,

64 See, for example, Animal Defenders International v. the United Kingdom, *op. cit.*, § 114.

65 Judgement of the ECtHR of 10 October 2013 on the case of Delfi AS v. Estonia, application no. 64569/09, § 87.

66 Directive 2000/31 / EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

objected, among other things, to the objective liability imposed by the Hungarian courts on the applicant company in this case, because it made any balancing between the competing rights, i.e. the right to reputation of the political party (Jobbik) and the right to freedom of expression of the applicant company, impossible. According to the Court, 'such objective liability may have foreseeable negative consequences on the flow of information on the Internet, impelling article authors and publishers to refrain altogether from hyperlinking to material over whose changeable content they have no control. This may have, directly or indirectly, a chilling effect on freedom of expression on the Internet.'[67] An even stronger comment on this can be found in the concurring opinion of Judge Pinto de Albuquerque, who observed that 'the Web is not intended, as a technology, to function in the way the respondent Government states, where spreading information via a hyperlink is itself always a "thought-content". This approach begs the question of how people are to convey information across the estimated trillions of web pages in existence today and countless future pages if doing so can give rise to liability. It is too burdensome, and in many cases impossible, for people to make a legal determination as to whether each and every hyperlinked content is defamatory or otherwise unlawful. If such a burden were to be imposed automatically on journalists, by way of an objective liability regime, it would stifle the freedom of the press. To paraphrase the words of Berners-Lee, hyperlinks are critical not merely to the digital revolution but to our continued prosperity – and even our liberty. Like democracy itself, they need defending.'[68] Considering this, the Court found the contested measure to be a disproportionate restriction on the right to freedom of expression.[69]

In a case concerning a similar issue, namely Editorial Board of PravoyeDelo and Shtekel v. Ukraine, the Court extended its doctrine of positive obligations into the area of the Internet. The case concerned the publication by an applicant of an anonymous letter, downloaded from a news website, which contained allegations of unlawful and corrupt activities by one of the senior officials of the Odessa Regional Department of the Security Service. The ECtHR found the rulings of the national courts against the applicants in the defamation case to be a violation of Article 10, the reason being, among others, that 'given the lack of adequate safeguards in the domestic law for journalists using information obtained from the Internet, the applicants could not foresee to the appropriate degree the consequences which the impugned publication might entail'. The interference was thus not prescribed by

67 Judgement of the ECtHR of 4 March 2019 on the case of Magyar JetiZrt v. Hungary, application no. 11257/16, § 83.

68 The concurring opinion of Judge Pinto de Albuquerque in *ibidem*, § 26.

69 *Ibidem*, § 84.

law.[70] Moreover, the ECtHR observed that 'having regard to the role the Internet plays in the context of professional media activities and its importance for the exercise of the right to freedom of expression generally… the Court considers that the absence of a sufficient legal framework at the domestic level allowing journalists to use information obtained from the Internet without fear of incurring sanctions seriously hinders the exercise of the vital function of the press as a "public watchdog"'.[71] Thus a regulatory framework is needed to ensure the effective protection of journalists' freedom of expression on the Internet, and states have a positive obligation under the Convention to provide it.[72]

4. The Protection of Private Life and the Internet

As was already mentioned, the Strasbourg Court, at least for a certain period of time, did not seem to be much in favour of the right to forget on the Internet, treating it rather as a limitation on the public's access to information available on the Internet, although, as was mentioned, this position has changed in the most recent case law. However, this does not mean that privacy as such is not protected in Strasbourg case law. It has been confirmed in Strasbourg case law that personal information which individuals can legitimately expect should not be published without their consent is protected under Article 8 of the ECHR; this also applies to the publication of a photograph.[73] One of the important aspects of private life in the context of the Internet is the protection of personal data. According to the Strasbourg Court, 'the protection of personal data is of fundamental importance to a person's enjoyment of his right to respect for private and family life'.[74] States have a positive obligation to ensure an effective deterrent against grave acts to a person's personal data, in some cases sometimes by means of efficient criminal-law provisions.[75] Moreover, positive obligations inherent in an effective respect for private or family life may involve the adoption of measures by the state designed to secure respect for private life even in the sphere of relations of individuals between themselves, for example an Internet user and those who provide access to a particular website.[76]

70 Judgement of the ECtHR of 5 May 2011 on the case of Editorial Board of PravoyeDelo and Shtekel v. Ukraine, application no. 33014/05, § 66.
71 *Ibidem*, § 64.
72 See Internet: Case-law, *op. cit.*, p. 17.
73 Judgement of the ECtHR of 12 October 2010 on the case of Saaristo and Others v. Finland, application no. 184/06, § 61.
74 Judgement of the ECtHR of 4 December 2008 on the case of S. and Marper v. the United Kingdom, application nos. 30562/04 and 30566/04, § 103.
75 See Internet: Case-law, *op. cit.*, p. 9.
76 *Ibidem*, p. 24.

The concept of the positive obligations of a state as regards the protection of privacy on the Internet was developed in the case of K.U. v. Finland concerning an advertisement of a sexual nature posted about a 12-year-old boy on an Internet dating site. The police and the courts could, however, under Finnish legislation at the time, require the Internet provider to identify the person who had posted the advertisement; the service provider, refusing to identify the person responsible, claimed it would constitute a breach of confidentiality. In its judgement in this case, the Court found a violation of Article 8 of the Convention, stating 'practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement'.[77] The ECtHR also pointed out that although freedom of expression and confidentiality of communications 'are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others'.[78] The positive obligations in this context mean that the legislator has the task 'to provide the framework for reconciling the various claims which compete for protection in this context. Such framework was not, however, in place at the material time, with the result that Finland's positive obligation with respect to the applicant could not be discharged.'[79]

As was already mentioned, the Court confirmed that the risk of harm to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, posed by content and communications on the Internet is certainly higher than that posed by the press.[80] Taking this, as well as the need to protect private life, into account, 'the policies governing reproduction of material from the printed media and the Internet may differ', and there is no absolute right to reproduce information already published on the Internet.[81] The higher risk is also connected with the ease with which information, even some personal information which is not initially meant to be posted online, may be picked up by third parties and discussed on the Web to the detriment of the individual's right to protection of private life.[82]

The Court is aware of particular threats to the protection of private life on the Internet connected with the availability and the circulation of information. In the case of Delfi AS v. Estonia, the Court admitted it is mindful 'of the importance of the

77 K.U. v. Finland, *op. cit.*, § 49.
78 *Ibidem*.
79 *Ibidem*.
80 Editorial Board v. Ukraine, *op. cit.*, § 63.
81 See Internet: Case-law, *op. cit.*, p. 30.
82 *Ibidem*, p. 16.

wishes of Internet users not to disclose their identity in exercising their freedom of expression. At the same time, the spread of the Internet and the possibility – or for some purposes the danger – that information once made public will remain public and circulate forever, calls for caution.'[83] What is also a specific feature of the Internet is how relatively easy it is to disclose information there. As a result, it is a difficult task to detect defamatory statements and remove them, given also the substantial amount of information there.[84]

Threats to private life are also posed by the monitoring of telephone calls, e-mail correspondence and Internet usage. In the Copland v. the UK case, such monitoring was carried out by the employer of the applicant. In this case, the Court found that it was irrelevant that the data held by the employer were not disclosed or used against the employee her in disciplinary or other proceedings, as just storing the data amounted to an interference with the applicant's private life. Finding a violation of Article 8 of the Convention, the Court pointed out that there was no domestic law regulating monitoring at the relevant time, so the alleged interference in this case was not 'in accordance with the law' as required by Article 8 Section 2 of the Convention. However, the Court would not exclude the monitoring of an employee's telephone, e-mail or Internet usage at the place of work if such monitoring may be considered 'necessary in a democratic society' in certain situations in pursuit of a legitimate aim.[85]

A person's right to the protection of his or her reputation, protected under Article 8 as part of the right to respect for private life, may be violated by comments posted on Internet forums. However, as the judgement on the case of Høiness v. Norway demonstrates, the Court does not always find a violation of Article 8. The case in question concerned an allegation connected with the Norwegian courts' refusal to impose civil liability on an Internet forum host after vulgar comments about the applicant had been posted on the forum. The Court mentioned that in order for Article 8 of the Convention to become applicable, 'the attack on personal honour and reputation must attain a certain level of seriousness and must have been carried out in a manner causing prejudice to personal enjoyment of the right to respect for private life'.[86] As such a level was not reached in this case, the Court found ambiguously, referring to its controversial margin of appreciation doctrine, that the national courts had acted within their margin of appreciation. They did so 'when seeking to establish

83 Delfi AS v. Estonia, *op. cit.*, § 92.

84 *Ibidem*.

85 Judgement of the ECtHR of 3 April 2007 on the case of Copland v. the United Kingdom, application no. 62617/00, § 48.

86 Judgement of the ECtHR of 19 March 2019 on the case of Høiness v. Norway, application no. 43624/14, § 64.

a balance between the applicant's rights under Article 8 and the news portal and host of the debate forums' opposing right to freedom of expression under Article 10'.[87]

Conclusions

Internet-related cases are a good illustration of how the Strasbourg Court has to deal with issues arising out of technological progress while giving its judgements on the basis of the Convention which is more than 70 years old. It is thus no wonder, as has been observed, that according to the ECtHR, the Convention is to be seen as 'a living instrument which must be interpreted in the light of present-day conditions'.[88] This approach of the Court to the interpretation of the Convention has turned out to be particularly useful and important in deciding Internet-related cases in Strasbourg. It has allowed the ECtHR to address a number of specific challenges resulting from the necessity of the protection of Convention rights in the context of the Internet, such as, for example, the issues of the liability of owners of Internet portals for defamatory comments, the liability for content hyperlinked in articles published online or the obligation of Internet service providers to disclose the identity of persons who post potentially criminal content.

The striking feature of Strasbourg's case law is the ECtHR's recognition of the considerable importance of the Internet for the exercise of freedom of expression and, in particular, freedom to seek and access information. Although the ECtHR regards the Internet as a communication medium, however, it recognises its specific features which affect the performance of rights protected by the Convention. The Internet has been evaluated by the Court from the perspective of both its beneficial impact on the exercise of some protected rights, in particular freedom to receive information, as well as some of its potentially adverse effects on the exercise of some other rights, such as rights to privacy. Calling the Internet 'one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas',[89] the Strasbourg Court appears to particularly appreciate its significance as regards the enhancing of the public's access to news and facilitating the dissemination of information in general, in particular in connection with 'its capacity to store and communicate vast amounts of information'.[90] At the same time, as the Court observed, the risk of damage which may be caused to the exercise and enjoyment of human rights, and particularly the right to respect for private life, by content and

87 *Ibidem*, § 75.
88 See T. Murphy and G. O Cuinn, Works in Progress: New Technologies and the European Court of Human Rights, 'Human Rights Law Review' 2010, vol 10, no. 4, p. 635.
89 Cengiz and Others v. Turkey, *op. cit*., § 49.
90 Times Newspapers v. the United Kingdom, *op. cit.*, § 27.

communications on the Internet is certainly higher than that posed, for example, by the press.

As has been demonstrated throughout the above analysis, the technological progress exemplified by the emergence of the Internet has had a number of implications as regards the protection of human rights under the ECHR. These implications include the 'new' rights connected with the Internet, such as the right of access to the Internet or the right to be forgotten. The Court appears to be cautious as regards expressing the general recognition of such rights. For example, in cases concerning access to the Internet, blocking of Internet sites, even if it amounts to prior restraint, is not regarded by the ECtHR as incompatible per se with the Convention. Such blocking needs to meet certain requirements laid down in Strasbourg case law, however, and appears to be untenable if there are less restrictive and intrusive measures available for domestic authorities. Here, the necessity test involving the principle of proportionality plays an important role. Therefore, states usually fail to comply with the requirements of necessity and proportionality if restrictions on Internet access are considered to be a drastic limitation of freedom of expression. Such restrictions are treated as the measure of last resort which have to be supported by very convincing reasons.

The position of the Court towards such new rights is also evolving. A good example is offered by the right to be forgotten. Here, the ECtHR was inclined to rule rather in favour of freedom of expression, indicating the importance of the Internet as a tool for enhancing the public's access to information and its dissemination, for example in the case of M.L. and W.W. v. Germany. Thus the interest in uninhibited access to Internet archives by the public outweighed the interest of individuals in being forgotten on the Internet. However, as was mentioned, in its recent case law this position of the Strasbourg Court has shifted more in favour of the right to be forgotten, as was demonstrated in its judgement on the case of Hurbain v. Belgium.

Another important observation is that despite the specificity of Internet-related cases, the Court appears to decide these cases, as has been shown, by firmly applying the same general principles developed in its case law both under Article 8 of ECHR when it comes to the protection of privacy on the Internet as well as under Article 10 of ECHR when freedom of expression is involved. Certainly, the Internet-related case law of the Convention is in the process of constant development. The Strasbourg Court has proved that it is capable of dealing with Internet-related cases based on general Convention norms and using its well-developed interpretation techniques. The ECtHR undoubtedly faces the challenge of dynamically developing Convention standards in its growing Internet-related case law. It is important, however, that these new standards are shaped in line with the spirit of the Convention.

REFERENCES

Best M.L., Can the Internet Be a Human Right? (in:) S. Hick, E.F. Halpin and E. Hoskins (eds.), Human Rights and the Internet, New York 2000.

Decision of the ECtHR of 11 March 2014 as to the admissibility of the case of Akdeniz v. Turkey, application no. 20877/10.

Decision of the ECtHR of 18 October 2005 as to the admissibility of the case of Perrin v. the United Kingdom.

Directive 2000/31 / EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

Garlicki L. (ed.), Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I, Komentarz do artykułów 1–18, Warsaw 2010.

Flogartis S., Zwart T., Fraser J., The European Court of Human Rights and its Discontents. Turning Criticism into Strength, Cheltenham/Northampton 2013.

Gosztonyi G European Court of Human Rights: Internet Access as a Means of Receiving and Imparting Information and Ideas, "International Comparative Jurisprudence" 2020, vol. 6, no. 2, https://ojs.mruni.eu/ojs/international-comparative-jurisprudence/article/view/6292.

Human Rights Council: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement.

Human Rights Council: The promotion, protection and enjoyment of human rights on the Internet, 27 June 2016, https://www.article19.org/data/files/Internet_Statement_Adopted.pdf.

Internet: Case-law of the European Court of Human Rights, Council of Europe, 2011, updated June 2015, https://www.echr.coe.int/documents/research_report_internet_eng.pdf.

Kakavoulis K., The case Google Spain v. AEPD and Mario Costeja Gonzalez of the Court of Justice of the European Union: A Brief Critical Analysis, https://www.homodigitalis.gr/en/posts/2900.

Mik C., Charakter, struktura i zakres zobowiązań z Europejskiej Konwencji Praw Człowieka, „Państwo i Prawo" 1992, no. 4.

Murphy T. and O Cuinn G., Works in Progress: New Technologies and the European Court of Human Rights, "Human Rights Law Review" 2010, vol 10, no. 4.

Karska E. and Karski K., Introduction: Extraterritorial Scope of Human Rights, "International Community Law Review" 2015, vol. 17, no. 4–5.

Prebensen S.C., The Margin of Appreciation and Articles 9, 10 and 11 of the Convention, "Human Rights Law Journal" 1998, vol. 19, no. 1.

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, GE.11–13201, 16 May 2011, https://www2.ohchr.org/english/bodies/hrcouncil/docs/ 17session/A.HRC.17.27_en.pdf.

Jasmontaite L. and Hert P. de, Access to the Internet in the EU: A Policy Priority, a Fundamental, a Human Right or a Concern for eGovernment? "Brussels Privacy Hub Working Paper"

February 2020, vol. 6, no. 19, https://www.researchgate.net/publication/339860840_Access_to_the_Internet_in_the_EU_a_policy_priority_a_fundamental_a_human_right_or_a_concern_for_eGovernment.

Organization for Security and Co-operation in Europe, 'Freedom of Expression on the Internet: A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States', 15 December 2011, https://www.osce.org/files/f/documents/e/f/80723.pdf.

Rzucidło J., Prawo dostępu do internetu jako podstawowe prawo człowieka: Część I, „Kwartalnik Naukowy Prawo Mediów Elektronicznych" 2010, no. 2.

Szeghalmi V., Difficulties Regarding the Right to Be Forgotten in the Case Law of the Strasbourg Court, "Athens Journal of Law" 2018, vol. 4, no. 3.

Wiśniewski A., Koncepcja marginesu oceny w orzecznictwie Europejskiego Trybunału Praw Człowieka, Gdańsk 2008.

Zieliński M., Dostęp do Internetu jako prawo człowieka? W sprawie potrzeby nowej wolności w konstytucji Rzeczypospolitej Polskiej, „Przegląd Sejmowy" 2013, no. 4.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.07
Received: 20.04.2021
Accepted: 15.07.2021

Salvatore Antonello Parente
University of Bari 'Aldo Moro', Italy
salvatore.parente@uniba.it
ORCID ID: https://orcid.org/0000–0002-5426–9043

Artificial Intelligence and Taxation: Assessment and Critical Issues of Tax-Levy Models

Abstract: The phenomenon of artificial intelligence and robotics, which has been under investigation for several years, has given rise to new taxation models, which have opened a lively ethical and legal debate in the scientific and cultural community which has not yet subsided. This essay, analyzing the tax effects of the relationship between intelligent machines and humans in the light of the perspectives offered by the new economy and after verifying compatibility with the founding principles of the Italian legal system (first of all, the rule of 'ability to pay' pursuant to Article 53 of the Constitution), assesses new taxable cases and tax-levy techniques related to the applications of artificial intelligence, also in the light of the possible tax subjectivity of the robot, in an attempt to make a contribution, from a *de iure condendo* perspective, to the taxation dynamics concerning automated production processes.

Keywords: digital personality of the robot, electronic ability to pay**,** intelligent machines, taxation dynamics, tax-levy models

Introduction

In its current sense, the term 'artificial intelligence' (AI) refers to the use of sophisticated hardware and software systems equipped with cognitive abilities typical of a human being – such as perception, rational reasoning, interpretation of external data, self-learning and decision-making autonomy – and able to plan certain actions and autonomously pursue defined purposes, within the limits predetermined by the programmer.[1] The multiple methods of use, from a legal point of view, make the unitary analysis of the phenomenon complex: in some cases, automated systems and algorithms play an ancillary and serving role compared to traditional production structures; in others, however, they appear to be able to develop independently specific skills, including through self-learning and experience, taking on 'anthropomorphic' characteristics. Finally, there is no lack of intermediate systems which, while able to develop actions and relationships independently, do not always appear to be traceable to systematically tested models.[2]

As well as being the subject of investigation by experts of computer science, the spread of robotics and artificial intelligence – largely resulting from the development of technological knowledge and innovation – leads to a deep reflection on the ethical,[3]

1 F. Roccatagliata, Implicazioni fiscali legate allo sviluppo della tecnologia e alla gestione dei flussi di dati generati in via automatica, 'Rivista della Guardia di Finanza' 2019, no. 5, p. 1281; D. Canè, Intelligenza artificiale e sanzioni amministrative tributarie, (in:) S. Dorigo (ed.), Il ragionamento giuridico nell'era dell'intelligenza artificiale, Pisa 2020, p. 319.

2 A. Uricchio, Robot tax: modelli di prelievo e prospettive di riforma, 'Giurisprudenza italiana' 2019, no. 7, p. 1752; A. Uricchio, La fiscalità dell'intelligenza artificiale tra nuovi tributi e ulteriori incentivi, (in:) U. Ruffolo (ed.), Intelligenza artificiale. Il diritto, i diritti, l'etica, Milan 2020, pp. 497–499.

3 L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, B. Schafer, P. Valcke and E. Vayena, AI4People: An Ethical Framework for a Good AI Society. Opportunities, Risks, Principles and Recommendations, 'Minds and Machines' 2018, no. 28, p. 689ff.; R. Cingolani and D. Andresciani, Robots, macchine intelligenti e sistemi autonomi: analisi della situazione e delle prospettive, (in:) G. Alpa (ed.), Diritto e intelligenza artificiale, Pisa 2020, p. 45ff.; L. D'Avack, La Rivoluzione tecnologica e la nuova era digitale: problemi etici, (in:) U. Ruffolo (ed.), Intelligenza artificiale, *op. cit.*, p. 3ff.; P. Moro, Macchine come noi: Natura e limiti della soggettività robotica, (in:) U. Ruffolo (ed.), Intelligenza artificiale, *op. cit.*, p. 45ff; U. Pagallo, Etica e diritto dell'Intelligenza Artificiale nella governance del digitale: il Middle-out-Approach, (in:) U. Ruffolo (ed.), Intelligenza artificiale, *op. cit.*, p. 29ff; G. Sartor and F. Lagioia, Le decisioni algoritmiche tra etica e diritto, (in:) U. Ruffolo (ed.), Intelligenza artificiale, *op. cit.*, p. 81ff.; E. Grassi, Etica e intelligenza artificiale. Questioni aperte, Canterano 2020.

economic[4] and legal levels,[5] and also in relation to tax matters,[6] its having facilitated the exercise of economic activities and contributed to making significant changes to the organization of work, domestic life, daily social relations and the models of production of goods and provision of services, allowing for further income and cost savings.[7] The transformation of the processes of wealth production has also generated a new way of considering and perceiving the 'real' market, with evident repercussions in the economic and legal spheres, so as to make it no longer a simple physical place for the exchange of property rights, modulated on the interaction of supply and demand, but rather a boundless and liquid space in which to access, freely and without time restrictions, and to exchange any type of good (even digital ones), right

4 J. Rifkin, L'era dell'accesso. La rivoluzione della new economy, Milan 2001; A. Giaume (ed.), Intelligenza artificiale. Dalla sperimentazione al vantaggio competitivo, Milan 2018; A. Mandelli, Intelligenza artificiale e marketing. Agenti invisibili, esperienza, valore e business, Milan 2018; F. Pacilli, L'imprenditore del futuro. Come aumentare i profitti, ridurre i costi e velocizzare l'amministrazione grazie al potere dell'Intelligenza Artificiale, Rome 2019; A. Semoli, AI marketing. Capire l'intelligenza artificiale per coglierne le opportunità, Milan 2019.

5 B.G. Buchanan and T.E. Headrick, Some Speculations About Artificial Intelligence and Legal Reasoning, 'Stanford Law Review' 1970, no. 1, p. 40ff.; G. Corasaniti, Intelligenza artificiale e diritto: il nuovo ruolo del giurista, (in:) U. Ruffolo (ed.), Intelligenza artificiale, *op. cit.*, p. 395ff.; M. Costanza, L'AI: de iure condito e de iure condendo, (in:) U. Ruffolo (ed.), Intelligenza artificiale, *op. cit.*, p. 407ff.; D. de Kerchove, Algoritmo, big data e sistema legale, (in:) A.F. Uricchio, G. Riccio and U. Ruffolo (eds.), Intelligenza Artificiale tra etica e diritti. Prime riflessioni a seguito del libro bianco dell'Unione europea, Bari 2020, p. 73ff.; S. Pietropaoli, Fine del diritto? L'intelligenza artificiale e il futuro del giurista, (in:) S. Dorigo (ed.), Il ragionamento giuridico, *op. cit.*, Pisa 2020, p. 107ff.; G. Romano, Diritto, robotica e teoria dei giochi: riflessioni su una sinergia, (in:) G. Alpa (ed.), Diritto e intelligenza artificiale, *op. cit.*, p. 103ff.; R. Rovatti, Il processo di apprendimento algoritmico e le applicazioni nel settore legale, (in:) U. Ruffolo (ed.), XXVI Lezioni di Diritto dell'Intelligenza Artificiale, Torino 2021, p. 31ff.

6 S. Dorigo, Intelligenza artificiale e norme antiabuso: il ruolo dei sistemi 'intelligenti' tra funzione amministrativa e attività giurisdizionale, 'Rassegna tributaria' 2019, no. 4, p. 728ff.; T. Rosembuj, Inteligencia artificial e impuesto, Barcelona 2019; L. Quarta, Impiego di sistemi IA da parte di amministrazioni finanziarie ed agenzie fiscali. Interesse erariale versus privacy, trasparenza, proporzionalità e diritto di difesa, (in:) A.F. Uricchio, G. Riccio, U. Ruffolo (eds.), Intelligenza Artificiale, *op. cit.*, p. 250ff.; A. Di Pietro, Leva fiscale e divisione sociale del lavoro, (in:) U. Ruffolo (ed.), XXVI Lezioni, *op. cit.*, p. 449ff.; V. Mastroiacovo, Uguaglianza sostenibile e sostegno all'innovazione: quale tassazione dei sistemi di intelligenza artificiale?, (in:) V.V. Cuocci, F.P. Lops and C. Motti (eds.), La circolazione della ricchezza nell'era digitale, Pisa 2021, p. 63ff.; A. Uricchio, Prospettive per l'introduzione di nuovi modelli di prelievo in materia di intelligenza artificiale anche alla luce del recovery plan, (in:) U. Ruffolo (ed.), XXVI Lezioni, *op. cit.*, p. 435ff.

7 S.A. Parente, Artificial Intelligences and 'Robot Tax': The Role of Robotics on Tax Structures and de iure condendo Perspectives, (in:) I. Florek, A. Koroncziová and J.L. Zamora Manzano (eds.), Crisis as a Challenge for Human Rights, Bratislava 2020, p. 353ff.

to enjoyment – even if only temporary and shared (the so-called 'sharing economy')[8] – and information (which, in this context, become legally relevant entities)[9].

In the current socio-economic structure, artificial intelligence and robotics both have the potential to rise to situations capable of generating manifestations of wealth attributable both to traditional categories (income, consumption, spending savings) as well as to completely new cases (the value of facilities deriving from the socialization of robotics).[10]

1. The New Economy and Tax-Levy Models

Whenever there is a new phenomenon, even if only in embryonic form, which can be abstractly configured as a centre for the imputation of rights and obligations, tax law is one of the most relevant sectors of legal knowledge to fathom its potential in order to verify its tax implications.[11]

An authoritative proposal, put forward by Bill Gates on 17 February 2017 during an interview with Quartz magazine,[12] aims to subject robotics to the imposition of taxes through the provision of special collection tools, in order to allow a moderate transition to new production models and compensate for the lower revenue which results from the processes of the automation of work.[13] In this light, it does not seem superfluous to ask whether the term 'work', which is relevant from the tax point of view, should be limited to a traditional meaning,[14] a human activity carried out

8 On this topic, see M. Allena, The Web Tax and Taxation of the Sharing Economy: Challenges for Italy, 'European Taxation' 2017, no. 7, p. 1ff.; C. Buccico, Modelli fiscali per la sharing economy, (in:) D. Di Sabato and A. Lepore (eds.), Sharing economy. Profili giuridici, Naples 2018, p. 161ff.; A. Uricchio and W. Spinapolice, La corsa ad ostacoli della web taxation, 'Rassegna tributaria' 2018, no. 3, p. 483ff.; R. Schiavolin, La tassazione della sharing economy attuata con piattaforme digitali, 'Rivista della Guardia di Finanza' 2019, no. 5, p. 1259ff.

9 A.F. Uricchio, Manuale di diritto tributario, Bari 2020, pp. 29–30.

10 A. Uricchio, La fiscalità, *op. cit*., p. 489ff.

11 R. Cordeiro Guerra, L'intelligenza artificiale nel prisma del diritto tributario, (in:) S. Dorigo (ed.), Il ragionamento giuridico, *op. cit*., p. 87.

12 K.J. Delaney, The robot that takes your job should pay taxes, says Bill Gates, https://qz.com/911968/bill-gates-the-robot-that-takes-your-job-should-pay-taxes/ (accessed 17.02.2017). For an initial discussion, see G. Fransoni, Per la chiarezza delle idee su Bill Gates e la tassazione dei robot, 'Rivista di diritto tributario – supplemento online' 10 March 2017, p. 1ff.

13 L. Summers, Robots are Wealth Creators and Taxing Them is Illogical, 'Financial Times' 5 March 2017; S. Dorigo, La tassa sui robot tra mito (tanto) e realtà (poca), 'Corriere tributario' 2018, no. 30, p. 2364; F. Roccatagliata, Implicazioni fiscali, *op. cit*., pp. 1283–1284; A. Uricchio, Robot tax, *op. cit*., p. 1750; A. Uricchio, La fiscalità, *op. cit*., pp. 494–495.

14 M. Persiani, Contratto di lavoro e organizzazione, Padua 1966, p. 5ff.; U. Prosperetti, Lavoro (fenomeno giuridico), (in:) Enciclopedia del diritto, vol. 23, Milan 1973, p. 332ff.; G. Suppiej, Il rapporto di lavoro: costituzione e svolgimento, Padua 1982, p. 96ff.; M. Grandi, Rapporto di lavoro, (in:) Enciclopedia del diritto, vol. 38, Milan 1990, p. 313ff.; C. Cester, G. Suppiej, Rapporto

through the use of physical and intellectual energy to gain an economic advantage and produce personal satisfaction, or rather if the activity rendered by intelligent robots can also be considered as work in a postmodern conception.[15] According to a classical conception,[16] work poses as a legal environment suitable for the production of taxable wealth only if it relates to human conduct; from a *de iure condendo* perspective, however, it would be desirable (albeit timidly, amid mistrust, scepticism –common to any new tax measure[17] – and perplexity) to rethink and overhaul the traditional models of levy, enhancing the forms of wealth expressed by new technologies and different types of artificial intelligence so as to subject the activities carried out by robots to taxation, based on the economic benefits enjoyed by the user.[18]

The preparation of tax measures aimed at targeting the forms of wealth created or manifested through the use of new technologies also appears essential in order to favour an overall rethinking of the tax models to be applied to the new economy and to guarantee an economic–financial balance,[19] which is elevated in the Italian legal system to a constitutional principle (Article 81 Paragraph 1 of the Constitution) with the changes made by constitutional law on 20 April 2012, no. 1.[20]

---

di lavoro, (in:) Digesto delle discipline privatistiche, sezione commerciale, vol. 12, Turin 1996, p. 10ff.; P. Tosi, F. Lunardon, Subordinazione, (in:) Novissimo digesto italiano, vol. 15, Turin 1998, p. 256ff.; M. Persiani, G. Prola, Contratto e rapporto di lavoro, Padua 2001, p. 3ff.

15 On this topic, see R. Del Punta, I diritti del lavoro nell'economia digitale, (in:) S. Dorigo (ed.), Il ragionamento giuridico, p. 99ff.

16 A. Uricchio, Il reddito dei lavori tra autonomia e dipendenza, Bari 2006, p. 47ff.; A.F. Uricchio, Percorsi di diritto tributario, Bari 2017, p. 157ff.; A.F. Uricchio, Manuale, *op. cit.*, p. 199ff.

17 A. Uricchio, La fiscalità, *op. cit*., p. 503ff.

18 A. Uricchio, Robot tax, *op. cit.*, p. 1754.

19 F. Bilancia, Note critiche sul c.d. 'pareggio di bilancio', 'Rivista trimestrale di diritto tributario' 2012, no. 2, p. 350ff.; D. Cabras, Su alcuni rilievi critici al c.d. 'pareggio di bilancio', 'Rivista AIC' 2012, no. 2, p. 1ff.; D. Morgante, La costituzionalizzazione del pareggio di bilancio, 'Federalismi.it' 2012, no. 14, p. 1ff.; G. Rivosecchi, Il c.d. pareggio di bilancio tra Corte e Legislatore, anche nei suoi riflessi sulle regioni: quando la paura prevale sulla ragione, 'Rivista AIC' 2012, no. 3, p. 1ff.; M. Bergo, Pareggio di bilancio 'all'italiana': Qualche riflessione a margine della Legge 24 dicembre 2012, n. 243 attuativa della riforma costituzionale più silenziosa degli ultimi tempi, 'Federalismi.it' 2013, no. 6, p. 22ff.; G.M. Napolitano, I nuovi limiti all'autonomia finanziaria degli Enti territoriali alla luce del principio del pareggio di bilancio, 'Rivista giuridica del Mezzogiorno' 2013, nos. 1–2, p. 91ff.; E. De Mita, Il conflitto tra capacità contributiva ed equilibrio finanziario dello Stato, 'Rassegna tributaria' 2016, no. 3, p. 563ff.

20 A. Uricchio, Robot tax, *op. cit.*, p. 1753; A. Uricchio, La fiscalità, *op. cit*., pp. 501–512.

2. The 'Electronic Ability to Pay' and Taxable Cases in the Automated Production Processes

The search for new taxable cases,[21] compared to those traditionally subject to taxation, in addition to not being arbitrary, must express the eligibility of the obliged subject's contribution according to economically appreciable situations, in compliance with the principles of reasonableness and fair distribution that derive from the tenet of the ability to pay and that make up the ethological humus at the basis of the Constitution of the Italian Republic.[22] For tax liability purposes, in addition to ascertaining whether artificial intelligences, as machines equipped with cognitive skills similar to a human, have their own tax subjectivity, it is necessary to verify their compatibility with the principle of ability to pay,[23] the foundation and limit of taxation and a guarantee for the taxpayer.[24]

From a distributive point of view, the tax burden – far from being limited only to indices (direct and indirect) that reveal wealth (such as income, assets and related increases, consumption or acts of exchange), from which can be deduced the suitability of the assumption to provide the tools with which to face the payment of the tax[25] – can affect any fact with an economic content, not necessarily of a financial nature, suitable for satisfying simple needs and interests or consisting of capacities, circumstances and events[26], from which the subjective eligibility to assume the tax obligation is rationally deductible.[27] This is the case of social position, i.e. the greater or lesser status of family well-being or education or the advantageous situation

21 A. Giovannini, Quale capacità contributiva? 'Diritto e pratica tributaria' 2020, no. 3, p. 839ff.

22 A.F. Uricchio, Percorsi, *op. cit.*, p. 41ff.; A. Uricchio, Robot tax, *op. cit.*, p. 1758; A. Uricchio, La fiscalità, *op. cit*., pp. 513–514; A.F. Uricchio, Manuale, *op. cit.*, pp. 50–51.

23 N. d'Amati, Diritto tributario. Teoria e critica, Turin 1985, p. 82.

24 A. Uricchio, Robot tax, *op. cit.*, pp. 1758–1759; A. Uricchio, La fiscalità, *op. cit*., p. 515.

25 For a constrasting view, see G. Falsitta, Il doppio concetto di capacità contributiva, 'Rivista di diritto tributario' 2004, nos. 7–8/I, p. 889ff.; F. Moschetti, Il principio di capacità contributiva, espressione di un sistema di valori che informa il rapporto tra singolo e comunità, (in:) L. Perrone and C. Berliri (eds.), Diritto tributario e Corte costituzionale, Naples 2006, p. 44ff.; G. Gaffuri, Il senso della capacità contributiva, (in:) L. Perrone and C. Berliri (eds.), Diritto tributario, *op. cit.*, p. 31ff.; I. Manzoni and G. Vanz, Il diritto tributario. Profili teorici e sistematici, Turin 2008, p. 30ff.; G. Gaffuri, Diritto tributario. Parte generale e speciale, Vicenza 2016, p. 32.

26 A. Fedele, Appunti dalle lezioni di diritto tributario, Turin 2005, p. 31ff.; A. Fedele, La funzione fiscale e la 'capacità contributiva' nella Costituzione italiana, (in:) L. Perrone and C. Berliri (eds.), Diritto tributario, *op. cit.*, p. 1ff.; A. Fedele, Diritto tributario (principi), (in:) Enciclopedia del diritto, Annali, vol. 2, part 2, Milan 2009, p. 447ff.; F. Gallo, Le ragioni del fisco. Etica e giustizia della tassazione, Bologna 2011, p. 78ff.; F. Gallo, L'evoluzione del sistema tributario e il principio di capacità contributiva, (in:) L. Salvini and G. Melis (eds.), L'evoluzione del sistema fiscale e il principio di capacità contributiva, Padua 2014, p. 3ff.; A. Fedele, Ancora sulla nozione di capacità contributiva nella costituzione italiana e sui 'limiti' costituzionali all'imposizione, (in:) L. Salvini and G. Melis (eds.), L'evoluzione, *op. cit.*, p. 13ff.

27 A. Uricchio, La fiscalità, *op. cit*., p. 513.

enjoyed by the originator of a negative externality compared to a similar activity without the aforementioned impact. This also admits to the owners of goods or activities that the taxation of their income, assets or consumption is unsatisfactory in relation to the advantageous situation connected to this ownership.[28]

So that the tax subjectivity of intelligent robots is recognized, it is necessary to identify an ability to pay – for them – that can be subject to taxation (a so-called 'electronic ability to pay')[29] autonomously and unitarily appreciable. From a *de iure condendo* perspective, depending on how the tax legislator intends to define the taxable case, the ability to pay could (in the abstract) be identified by the asset value of the robot, by the production of the income deriving from the activity carried out by the same (and, therefore, in the greater production capacity deriving from the use of robotics and automated processes)[30] or in the cost savings achieved through its use.[31]

However, it would not be possible to make the simple existence of the robot relate to a wealth index to legitimize the provision of an 'electronic capitation' or a 'possession tax': taxes of this kind could prove unfair if applied in an equal and generalized manner for all robots without taking into account their value, the time of use, their effective production capacity and, therefore, the utility resulting from their use.[32]

3. Fiscal Policies and Robot Tax: De Iure Condendo Perspectives and Critical Issues of the Models

From an equalization point of view, the robot tax, as a form of levy imposed on automated production processes, can take on different configurations, depending on the tax policy choices made by the individual legal system: on the one hand, it could substantiate itself in the denial of tax concessions on investments aimed at automating production or relating to economic operators who make a large part of their profits using robotic tools or technological innovation processes; on the other hand, it could consist in the preparation of a real tax applied to the 'robotic person', on the basis of the 'normal value' of the activity performed (*rectius*, fictitious remuneration obtained following comparison with human work), as an entity deemed to have autonomous

28 R. Cordeiro Guerra, L'intelligenza artificiale, *op. cit.*, pp. 92–93.

29 X. Oberson, Taxer les robots? L'émergence d'une capacité contributive électronique, 'Pratique juridique actuelle' 2017, no. 2, p. 232ff.

30 S. Dorigo, La tassa sui robot, *op. cit.*, p. 2369.

31 A.F. Uricchio, Manuale, *op. cit.*, p. 61ff.

32 A. Uricchio, Robot tax, *op. cit.*, p. 1760; A. Uricchio, La fiscalità, *op. cit*., pp. 518–519.

legal subjectivity[33] (a so-called 'electronic personality')[34] and learning capacity (so-called 'machine learning'), and able to perform functions and carry out actions previously reserved only to human beings.[35]

In reality, both of the proposed solutions raise critical issues: the first variant, in the absence of uniform supranational regulation, would not be fully effective, as economic operators could easily escape a disincentivizing tax regime by delocalizing production to jurisdictions which, in order to attract capital and taxable matter, are free of such obstacles.[36] The second model, undoubtedly striking, appears entirely theoretical at the moment, as it is not certain that technological developments can, at least in the short term, create a 'thinking' machine equipped with its own decision-making autonomy and tax subjectivity, even in problems of a dogmatic nature which pertain both to the subjective profile (lacking a shared notion of 'robot' and a level of autonomy such as to allow a separate consideration from human beings) and to the objective side (since it is not easy to identify the elements capable of justifying the robot's contribution to public expenses, due to the absence of a salary to which to parameterize the ability to pay).[37]

33 X. Oberson, Taxing Robots? From the Emergence of an Electronic Ability to Pay to a Tax on Robots or the Use of Robots, 'World Tax Journal' May 2017, p. 247; F. Caroccia, Soggettività giuridica dei robot? (in:) G. Alpa (ed.), Diritto e intelligenza artificiale, *op. cit.*, p. 213ff.; A. Berti Suman, Intelligenza artificiale e soggettività giuridica: quali diritti (e doveri) dei robot? (in:) G. Alpa (ed.), Diritto e intelligenza artificiale, *op. cit.*, p. 251ff.; P. Moro, Alle frontiere della soggettività: indizi di responsabilità delle macchine intelligenti, (in:) U. Ruffolo (ed.), XXVI Lezioni, *op. cit.*, p. 55ff.

34 European Parliament Resolution of 16 February 2017 concerning recommendations to the Commission on civil law rules on robotics, 2015/2103/(INL), § 59(f), https://eur-lex.europa.eu/legal-content/IT/ALL/?uri= CELEX%3A52017IP0051 (accessed 16.09.2020); U. Ruffolo, Intelligenza artificiale, machine learning e responsabilità da algoritmo, 'Giurisprudenza italiana' 2019, no. 7, p. 1702ff.; G. Teubner, Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi, ed. P. Femia, Naples 2019, p. 29; U. Ruffolo, La 'personalità elettronica', (in:) U. Ruffolo (ed.), Intelligenza artificiale, *op. cit.*, Milan 2020, p. 213ff.; U. Ruffolo, Responsabilità da algoritmo e 'personalità elettronica', (in:) A.F. Uricchio, G. Riccio and U. Ruffolo (eds.), Intelligenza Artificiale, *op. cit.*, p. 365ff.; U. Ruffolo, La personalità elettronica tra 'doveri' e 'diritti' della machina, (in:) U. Ruffolo (ed.), XXVI Lezioni, *op. cit.*, p. 115ff. For criticism, see A. Drigo, Sistemi emergenti di Intelligenza Artificiale e personalità giuridica: un contributo interdisciplinare alla tematica, (in:) S. Dorigo (ed.), Il ragionamento giuridico, *op. cit.*, p. 195.

35 S. Dorigo, La tassa sui robot, *op. cit.*, p. 2367.

36 J. Walker, Robot Tax: A Summary of Arguments 'For' and 'Against', https://emerj.com/ai-sector-overviews/robot-tax-summary-arguments/ (accessed 24.10.2017).

37 S. Dorigo, La tassa sui robot, *op. cit.*, p. 2367; T. Falcão, Should My Dishwasher Pay a Robot Tax? 'Tax Notes International' 2018, p. 1273ff.

4. The Attribution of Asset Relations to Intelligent Machines: The 'Digital Peculium' and 'Robot Companies'

The prospect of a future attribution of asset relations to intelligent machines is, moreover, the subject of lively debate: a positive solution could be endorsed by recalling and adapting the Romanistic institution of the *peculium*[38] – an object of multiple uses as a separate asset of the master managed independently by the slave, a simple *instrumentum vocale*[39] devoid of any form of legal subjectivity – which sought to outline the mechanisms of relative and contingent subjectivization of what was certainly not a juridically relevant subject for the law then in force.[40] The 'digital *peculium*' would make it possible to create a separation of assets – aimed at protecting the multiple interests involved – without the need to recall a full legal personality.[41]

On closer inspection, in the current phase, subjecting artificial intelligences to taxation is not the same as considering robots as taxable persons, since tax liability is limited to community members only, as they are the locus of the attribution of rights and duties of a political and tax-related nature. Although in the near future the inclusion of robots among the members of the community and the recognition that they have an electronic ability to pay,[42] limited to their ownership of assets or taxable wages (as hypothesized in a famous collection of science-fiction short stories written by Isaac Asimov),[43] cannot be excluded, it is certain that these conditions are not yet current, as the self-determination of automata appears premature.[44] In this light, a robot tax could become a toll on companies with a higher level of automation or with less use of human labour (so-called 'robot companies'), hitting the excess profits achieved thanks to the use of innovative technologies.[45]

38 N. Wiener, The Human Use of Human Beings. Cybernetics and Society, Boston 1950; G. Taddei Elmi, I diritti dell'intelligenza artificiale tra soggettività e valore: fantadiritto o ius condendum? (in:) L. Lombardi Vallauri (ed.), Il meritevole di tutela, Milan 1990, p. 685ff.; L.E. Wein, The Responsibility of Intelligent Artifacts: Toward an Automation Jurisprudence, 'Harvard Journal of Law & Technology' 1992, no. 6, p. 103ff.; U. Pagallo, The Laws of Robots. Crimes, Contracts and Torts, Cham 2013, p. 102ff.; M. Rizzuti, Il peculium del robot. Spunti sul problema della soggettivizzazione dell'intelligenza artificiale, (in:) S. Dorigo (ed.), Il ragionamento giuridico, *op. cit.*, p. 284.

39 F. Bianchini, A.M. Gliozzo and M. Matteuzzi, Instrumentum vocale: intelligenza artificiale e linguaggio, Bologna 2008; E. Stolfi, La soggettività commerciale dello schiavo nel mondo antico, 'Teoria e storia del diritto privato' 2009, no. 2, p. 1ff.; D. Di Sabato, Gli smart contracts: robot che gestiscono il rischio contrattuale, 'Contratto e impresa' 2017, no. 2, p. 389.

40 R. Cordeiro Guerra, L'intelligenza artificiale, *op. cit.*, pp. 91–92; M. Rizzuti, Il peculium del robot, *op. cit.*, p. 286.

41 A. Drigo, Sistemi emergenti, *op. cit.*, p. 196.

42 X. Oberson, Taxing Robots? *op. cit.*, p. 250.

43 I. Asimov, Io, robot, Milan 1950.

44 R. Cordeiro Guerra, L'intelligenza artificiale, *op. cit.*, p. 91.

45 G. Fransoni, Per la chiarezza delle idee, *op. cit.*, pp. 1–2.

At the most, due to the limits that, at present, do not allow the recognition of a tax subjectivity for intelligent machines, a solution to legitimize their taxation could be to elaborate the concept of the 'digital personality of the robot', taking up the proposals on the taxation of the digital economy which, in the matter of permanent establishment, refer to the existence of a 'significant digital presence': in this way, the robots would be subject to a levy not as autonomous taxable persons but as permanent establishments (with separate taxation) of their master and beneficial owner.[46]

5. Robot Tax, Strengthened Ability to Pay and Presumptive Forms of Taxation

From a postmodern processing perspective, there is no shortage of further alternatives that could be feasible in the abstract: on the one hand, the possibility of parameterising a robot tax to an index of 'strengthened ability to pay', consisting of the economic advantage – equal to the greater potential to generate revenues or cost savings (such as lower costs incurred for the replacement of employees) – consequent to the activity carried out by intelligent machines in a given tax period or relative to the utilities received, taxed on the basis of the normal value (with the provision of specific corrective measures) and aimed at preventing the double taxation of the company's profits and the economic benefits achieved by the robots used to carry out the production activity. On the other hand is the possibility of the use of presumptive taxation models, applied reasonably and based on the estimate of the benefits associated with the use of robots, also through an increase in the rates of direct taxes imposed on those who make use of the robotic workforce due to their greater capacity to produce profits.

Especially at first, it could be simpler to foresee an experimental tax on the asset of intelligent robots, differentiated according to their capacity for accumulating data and knowledge, and imposed on the user; this tax, insisting on a different assumption from that for income taxes, as well as allowing for greater revenue, would be easily ascertainable, being the presence of a robot which is traceable and recognizable.[47]

In reality, beyond the transitory experimentation, some solutions could lead to empirical or reductive results in the long term, as they relate the levy to the higher profit achieved through the use of automated procedures (so-called 'extra profits') or differentiate it based on the robot's learning ability; even making use of presumptive tax models would not always allow the quantification of exactly the contribution provided by the artificial intelligences.[48] Furthermore, subjecting the greater profits

46 F. Roccatagliata, Implicazioni fiscali, *op. cit.*, p. 1285ff.; A. Uricchio, La fiscalità, *op. cit*., p. 506, n. 48.

47 A. Uricchio, Robot tax, *op. cit.*, pp. 1760–1761; A. Uricchio, La fiscalità, *op. cit*., p. 521.

48 S. Dorigo, La tassa sui robot, *op. cit.*, pp. 2367–2368.

made by companies whose production system is based on automation to taxation with ordinary income taxes cannot always grasp the advantages that the availability of this form of organization of production brings to its owner in a satisfactory way.[49] From a *de iure condendo* perspective, there is the possibility of configuring the robot tax without excessively altering the structure of the existing tax system; using the tax instrument to compensate for the social damage caused by technological innovation, in order to take into account negative externalities, correlates to the automation of production processes in terms of employment and the financing of public spending.[50]

Conclusion

In this light, and taking up Pigouvian theory,[51] the taxation of robotics, even in the absence of certain scientific evidence, would affect the production of technological companies due to the negative external effects resulting from the adoption of automated procedures, since these are activities that pursue worthy objectives of economic growth, but with respect to which it is necessary to manage and internalize any negative collateral consequences so as to protect the community – in order to restore financial equilibrium through compensation for lower income, related to the reduction of human labour[52] – and the individuals affected by the loss of employment through the preparation of policies aimed at supporting the costs of training and retraining human personnel.

Substituting the negative externality to be compensated for with taxation of the decline in employment, the tax base could be parameterized to the reduction of the human workforce induced by the automation of production processes and, therefore, to the cost savings achieved by the economic operator, who no longer has to pay a salary to employees.[53] In this way, with regard to the distribution profile of the tax burden, the revenue that can be obtained from a robot tax would allow the imbalances produced by innovative policies within the labour market to be faced on the basis of a further reflection: the effects of automation require public intervention, as they cannot be remedied alone by the market's 'invisible hand'.[54]

49 R. Cordeiro Guerra, L'intelligenza artificiale, *op. cit.*, p. 93.

50 S. Dorigo, La tassa sui robot, *op. cit.*, pp. 2367–2368; R. Cordeiro Guerra, L'intelligenza artificiale, *op. cit.*, p. 90, n. 8, p. 92.

51 A.C. Pigou, Economia del benessere, Turin 1960.

52 F. Roccatagliata, Implicazioni fiscali, *op. cit.*, p. 1286.

53 S. Dorigo, La tassa sui robot, *op. cit.*, pp. 2368–2369.

54 G. Fransoni, Per la chiarezza delle idee, *op. cit.*, p. 2; S. Dorigo, La tassa sui robot, *op. cit.*, p. 2369; F. Gallo, Il futuro non è un vicolo cieco. Lo stato tra globalizzazione, decentramento ed economia digitale, Palermo 2019, p. 30ff.

A hybrid solution seems to be the one advanced in the Italian legal system (Article 1 of the law proposal C. 4621,[55] presented to the Chamber of Deputies on 3 August 2017 and not implemented), which, in order to discourage the replacement of the human workforce with robotics and to induce corporate companies to reconvert production processes, equipping workers with the knowledge and skills to guarantee them a place in a constantly evolving labour market,[56] has proposed a 1-percentage-point increase in the corporate tax rate in the event that 'the production activity of the company is carried out and managed mainly by artificial intelligence and robotics systems', unless the taxpayer provides investment of a sum equal to 0.5% of its revenues in professional retraining projects for its employees, or in corporate welfare instruments, in the related tax period.

The experimentation with tax tools applied to the innovations brought by robotics offers multiple solutions that the tax legislator is called to examine with particular caution;[57] however, the evaluation of the levy models used to assess artificial intelligence requires shared choices in the international context or, at least, in the European Union,[58] as recently reiterated in the European Commission's White Paper on Artificial Intelligence,[59] in order to avoid market distortions that could damage free-competition rules and prevent further reasons for the delocalization of production and wealth.

REFERENCES

Allena M., The Web Tax and Taxation of the Sharing Economy. Challenges for Italy, "European Taxation" 2017, no. 7.

Asimov I., Io, robot, Milan 1950.

Bergo M., Pareggio di bilancio 'all'italiana'. Qualche riflessione a margine della Legge 24 dicembre 2012, n. 243 attuativa della riforma costituzionale più silenziosa degli ultimi tempi, "Federalismi.it" 2013, no. 6.

55 See http://documenti.camera.it/_dati/leg17/lavori/stampati/pdf/17PDL0054410.pdf (accessed 16.09.2020).

56 L. Tomassini, Intelligenza artificiale, impresa, lavoro, (in:) U. Ruffolo (ed.), XXVI Lezioni, *op. cit.*, p. 43ff.; A. Vacchi, L'intelligenza artificiale nella produzione industriale: le ricadute sul mondo del lavoro, (in:) U. Ruffolo (ed.), XXVI Lezioni, *op. cit.*, p. 465ff.

57 A. Uricchio, La fiscalità, *op. cit*., pp. 523–528.

58 A.F. Uricchio, La sfida della strategia europea dell'Intelligenza Artificiale tra regolazione e tassazione, (in:) A.F. Uricchio, G. Riccio and U. Ruffolo (eds.), Intelligenza Artificiale, *op. cit.*, p. 193ff.

59 White Paper on Artificial Intelligence: A European Approach to Excellence and Trust, adopted by the European Commission on 19 February 2020 (COM(2020) 65 final), https://ec.europa.eu/info/sites/default/files/ commission-white-paper-artificial-intelligence-feb2020_it.pdf (accessed 16.09.2020). On this topic, see A.F. Uricchio, Prefazione, (in:) A.F. Uricchio, G. Riccio and U. Ruffolo (eds.), Intelligenza Artificiale, *op. cit.*, p. 17ff.

Berti Suman A., Intelligenza artificiale e soggettività giuridica: quali diritti (e doveri) dei robot?, (in:) G. Alpa (ed.), Diritto e intelligenza artificiale, Pisa 2020.

Bianchini F., Gliozzo A.M. and Matteuzzi M., Instrumentum vocale: intelligenza artificiale e linguaggio, Bologna 2008.

Bilancia F., Note critiche sul c.d. 'pareggio di bilancio', "Rivista trimestrale di diritto tributario" 2012, no. 2.

Buccico C., Modelli fiscali per la sharing economy, (in:) D. Di Sabato, A. Lepore (eds.), Sharing economy. Profili giuridici, Naples 2018.

Buchanan B.G. and Headrick T.E., Some Speculations About Artificial Intelligence and Legal Reasoning, "Stanford Law Review" 1970, no. 1.

Cabras D., Su alcuni rilievi critici al c.d. 'pareggio di bilancio', "Rivista AIC" 2012, no. 2.

Canè D., Intelligenza artificiale e sanzioni amministrative tributarie, (in:) S. Dorigo (ed.), Il ragionamento giuridico nell'era dell'intelligenza artificiale, Pisa 2020.

Caroccia F., Soggettività giuridica dei robot?, (in:) G. Alpa (ed.), Diritto e intelligenza artificiale, Pisa 2020.

Cester C. and Suppiej G., Rapporto di lavoro, (in:) Digesto delle discipline privatistiche, sezione commerciale, vol. XII, Turin 1996.

Cingolani R. and Andresciani D., Robots, macchine intelligenti e sistemi autonomi: analisi della situazione e delle prospettive, (in:) G. Alpa (ed.), Diritto e intelligenza artificiale, Pisa 2020.

Corasaniti G., Intelligenza artificiale e diritto: il nuovo ruolo del giurista, (in:) U. Ruffolo (ed.), Intelligenza artificiale. Il diritto, i diritti, l'etica, Milan 2020.

Cordeiro Guerra R., L'intelligenza artificiale nel prisma del diritto tributario, (in:) S. Dorigo (ed.), Il ragionamento giuridico nell'era dell'intelligenza artificiale, Pisa 2020.

Costanza M., L'AI: de iure condito e de iure condendo, (in:) U. Ruffolo (ed.), Intelligenza artificiale. Il diritto, i diritti, l'etica, Milan 2020.

d'Amati N., Diritto tributario. Teoria e critica, Turin 1985.

D'Avack L., La Rivoluzione tecnologica e la nuova era digitale: problemi etici, (in:) U. Ruffolo (ed.), Intelligenza artificiale. Il diritto, i diritti, l'etica, Milan 2020.

Delaney K.J., The robot that takes your job should pay taxes, says Bill Gates, https://qz.com/911968/bill-gates-the-robot-that-takes-your-job-should-pay-taxes/.

Del Punta R., I diritti del lavoro nell'economia digitale, (in:) S. Dorigo (ed.), Il ragionamento giuridico nell'era dell'intelligenza artificiale, Pisa 2020.

de Kerchove D., Algoritmo, big data e sistema legale, (in:) A.F. Uricchio, G. Riccio and U. Ruffolo (ed.), Intelligenza Artificiale tra etica e diritti. Prime riflessioni a seguito del libro bianco dell'Unione europea, Bari 2020.

De Mita E., Il conflitto tra capacità contributiva ed equilibrio finanziario dello Stato, "Rassegna tributaria" 2016, no. 3.

Di Pietro A., Leva fiscale e divisione sociale del lavoro, (in:) U. Ruffolo (ed.), XXVI Lezioni di Diritto dell'Intelligenza Artificiale, Turin 2021.

Di Sabato D., Gli smart contracts: robot che gestiscono il rischio contrattuale, "Contratto e impresa" 2017, no. 2.

Dorigo S., La tassa sui robot tra mito (tanto) e realtà (poca), "Corriere tributario" 2018, no. 30.

Dorigo S., Intelligenza artificiale e norme antiabuso: il ruolo dei sistemi 'intelligenti' tra funzione amministrativa e attività giurisdizionale, "Rassegna tributaria" 2019, no. 4.

Drigo A., Sistemi emergenti di Intelligenza Artificiale e personalità giuridica: un contributo interdisciplinare alla tematica, (in:) S. Dorigo (ed.), Il ragionamento giuridico nell'era dell'intelligenza artificiale, Pisa 2020.

European Parliament Resolution of February 16, 2017 concerning recommendations to the Commission on civil law rules on robotics [2015/2103/(INL)], https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A52017IP0051.

Falcão T., Should My Dishwasher Pay a Robot Tax?, "Tax Notes International" 2018.

Falsitta G., Il doppio concetto di capacità contributiva, 'Rivista di diritto tributario' 2004, no. 7–8, I.

Fedele A., Appunti dalle lezioni di diritto tributario, Turin 2005.

Fedele A., La funzione fiscale e la 'capacità contributiva' nella Costituzione italiana, (in:) L. Perrone and C. Berliri (eds.), Diritto tributario e Corte costituzionale, Naples 2006.

Fedele A., Diritto tributario (principi), (in:) Enciclopedia del diritto, Annali, vol. 2, part 2, Milan 2009.

Fedele A., Ancora sulla nozione di capacità contributiva nella costituzione italiana e sui 'limiti' costituzionali all'imposizione, (in:) L. Salvini and G. Melis (eds.), L'evoluzione del sistema fiscale e il principio di capacità contributiva, Padua 2014.

Floridi L., Cowls J., Beltrametti M., Chatila R., Chazerand P., Dignum V., Luetge C., Madelin R., Pagallo U., Rossi F., Schafer B., Valcke P. and Vayena E., AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles and Recommendations, "Minds and Machines" 2018, no. 28.

Fransoni G., Per la chiarezza delle idee su Bill Gates e la tassazione dei robot, "Rivista di diritto tributario - supplemento online" 10 March 2017.

Gaffuri G., Il senso della capacità contributiva, (in:) L. Perrone and C. Berliri (eds.), Diritto tributario e Corte costituzionale, Naples 2006.

Gaffuri G., Diritto tributario. Parte generale e speciale, Vicenza 2016.

Gallo F., Le ragioni del fisco. Etica e giustizia della tassazione, Bologna 2011.

Gallo F., L'evoluzione del sistema tributario e il principio di capacità contributiva, (in:) L. Salvini and G. Melis (eds.), L'evoluzione del sistema fiscale e il principio di capacità contributiva, Padua 2014.

Gallo F., Il futuro non è un vicolo cieco. Lo stato tra globalizzazione, decentramento ed economia digitale, Palermo 2019.

Giaume A. (ed.), Intelligenza artificiale. Dalla sperimentazione al vantaggio competitivo, Milan 2018.

Giovannini A., Quale capacità contributiva?, "Diritto e pratica tributaria" 2020, no. 3.

Grandi M., Rapporto di lavoro, (in:) Enciclopedia del diritto, vol. XXXVIII, Milan 1990.

Grassi E., Etica e intelligenza artificiale. Questioni aperte, Canterano 2020.

Mandelli A., Intelligenza artificiale e marketing. Agenti invisibili, esperienza, valore e business, Milan 2018.

Manzoni I. and Vanz G., Il diritto tributario. Profili teorici e sistematici, Turin 2008.

Mastroiacovo V., Uguaglianza sostenibile e sostegno all'innovazione: quale tassazione dei sistemi di intelligenza artificiale?, (in:) V.V. Cuocci, F.P. Lops and C. Motti (eds.), La circolazione della ricchezza nell'era digitale, Pisa 2021.

Morgante D., La costituzionalizzazione del pareggio di bilancio, "Federalismi.it" 2012, no. 14.

Moro P., Macchine come noi. Natura e limiti della soggettività robotica, (in:) U. Ruffolo (ed.), Intelligenza artificiale. Il diritto, i diritti, l'etica, Milan 2020.

Moro P., Alle frontiere della soggettività: indizi di responsabilità delle macchine intelligenti, (in:) U. Ruffolo (ed.), XXVI Lezioni di Diritto dell'Intelligenza Artificiale, Turin 2021.

Moschetti F., Il principio di capacità contributiva, espressione di un sistema di valori che informa il rapporto tra singolo e comunità, (in:) L. Perrone and C. Berliri (eds.), Diritto tributario e Corte costituzionale, Naples 2006.

Napolitano G.M., I nuovi limiti all'autonomia finanziaria degli Enti territoriali alla luce del principio del pareggio di bilancio, "Rivista giuridica del Mezzogiorno" 2013, no. 1–2.

Oberson X., Taxer les robots? L'émergence d'une capacité contributive èlectronique, "Pratique juridique actuelle" 2017, no. 2.

Oberson X., Taxing Robots? From the Emergence of an Electronic Ability to Pay to a Tax on Robots or the Use of Robots, "World Tax Journal" May 2017.

Pacilli F., L'imprenditore del futuro. Come aumentare i profitti, ridurre i costi e velocizzare l'amministrazione grazie al potere dell'Intelligenza Artificiale, Rome 2019.

Pagallo U., The Laws of Robots. Crimes, Contracts and Torts, Cham 2013.

Pagallo U., Etica e diritto dell'Intelligenza Artificiale nella governance del digitale: il Middle-out-Approach, (in:) U. Ruffolo (ed.), Intelligenza artificiale. Il diritto, i diritti, l'etica, Milan 2020.

Parente S.A., Artificial intelligences and "robot tax": the role of robotics on tax structures and de iure condendo perspectives, (in:) I. Florek, A. Koroncziová, J.L. Zamora Manzano (eds.), Crisis as a challenge for human rights, Bratislava 2020.

Persiani M., Contratto di lavoro e organizzazione, Padua 1966.

Persiani M., Prola G., Contratto e rapporto di lavoro, Padua 2001.

Pietropaoli S., Fine del diritto? L'intelligenza artificiale e il futuro del giurista, (in:) S. Dorigo (ed.), Il ragionamento giuridico nell'era dell'intelligenza artificiale, Pisa 2020.

Pigou A.C., Economia del benessere, Turin 1960.

Prosperetti U., Lavoro (fenomeno giuridico), (in:) Enciclopedia del diritto, vol. XXIII, Milan 1973.

Quarta L., Impiego di sistemi IA da parte di Amministrazioni finanziarie ed agenzie fiscali. Interesse erariale versus privacy, trasparenza, proporzionalità e diritto di difesa, (in:) A.F. Uricchio, G. Riccio and U. Ruffolo (eds.), Intelligenza Artificiale tra etica e diritti. Prime riflessioni a seguito del libro bianco dell'Unione europea, Bari 2020.

Rifkin J., L'era dell'accesso. La rivoluzione della new economy, Milan 2001.

Rivosecchi G., Il c.d. pareggio di bilancio tra Corte e Legislatore, anche nei suoi riflessi sulle regioni: quando la paura prevale sulla ragione, "Rivista AIC" 2012, no. 3.

Rizzuti M., Il peculium del robot. Spunti sul problema della soggettivizzazione dell'intelligenza artificiale, (in:) S. Dorigo (ed.), Il ragionamento giuridico nell'era dell'intelligenza artificiale, Pisa 2020.

Roccatagliata F., Implicazioni fiscali legate allo sviluppo della tecnologia e alla gestione dei flussi di dati generati in via automatica, "Rivista della Guardia di Finanza" 2019, no. 5.

Romano G., Diritto, robotica e teoria dei giochi: riflessioni su una sinergia, (in:) G. Alpa (ed.), Diritto e intelligenza artificiale, Pisa 2020.

Rosembuj T., Inteligencia artificial e impuesto, Barcelona 2019.

Rovatti R., Il processo di apprendimento algoritmico e le applicazioni nel settore legale, (in:) U. Ruffolo (ed.), XXVI Lezioni di Diritto dell'Intelligenza Artificiale, Turin 2021.

Ruffolo U., Intelligenza artificiale, machine learning e responsabilità da algoritmo, "Giurisprudenza italiana" 2019, no. 7.

Ruffolo U., La 'personalità elettronica', (in:) U. Ruffolo (ed.), Intelligenza artificiale. Il diritto, i diritti, l'etica, Milan 2020.

Ruffolo U., Responsabilità da algoritmo e 'personalità elettronica', (in:) A.F. Uricchio, G. Riccio and U. Ruffolo (a cura di), Intelligenza Artificiale tra etica e diritti. Prime riflessioni a seguito del libro bianco dell'Unione europea, Bari 2020.

Ruffolo U., La personalità elettronica tra 'doveri' e 'diritti' della machina, (in:) U. Ruffolo (ed.), XXVI Lezioni di Diritto dell'Intelligenza Artificiale, Turin 2021.

Sartor G. and Lagioia F., Le decisioni algoritmiche tra etica e diritto, (in:) U. Ruffolo (ed.), Intelligenza artificiale. Il diritto, i diritti, l'etica, Milan 2020.

Schiavolin R., La tassazione della sharing economy attuata con piattaforme digitali, "Rivista della Guardia di Finanza" 2019, no. 5.

Semoli A., AI marketing. Capire l'intelligenza artificiale per coglierne le opportunità, Milan 2019.

Stolfi E., La soggettività commerciale dello schiavo nel mondo antico, "Teoria e storia del diritto privato" 2009, no. 2.

Summers L., Robots Are Wealth Creators and Taxing Them Is Illogical, "Financial Times" 5 March 2017.

Suppiej G., Il rapporto di lavoro: costituzione e svolgimento, Padua 1982.

Taddei Elmi G., I diritti dell'intelligenza artificiale tra soggettività e valore: fantadiritto o ius condendum?, (in:) L. Lombardi Vallauri (ed.), Il meritevole di tutela, Milan 1990.

Teubner G., Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi, a cura di P. Femia, Naples 2019.

Tomassini L., Intelligenza artificiale, impresa, lavoro, (in:) U. Ruffolo (ed.), XXVI Lezioni di Diritto dell'Intelligenza Artificiale, Turin 2021.

Tosi P. and Lunardon F., Subordinazione, (in:) Novissimo digesto italiano, vol. XV, Turin 1998.

Uricchio A., Il reddito dei lavori tra autonomia e dipendenza, Bari 2006.

Uricchio A. and Spinapolice W., La corsa ad ostacoli della web taxation, "Rassegna tributaria" 2018, no. 3.

Uricchio A., Robot tax: modelli di prelievo e prospettive di riforma, 'Giurisprudenza italiana' 2019, no. 7.

Uricchio A., La fiscalità dell'intelligenza artificiale tra nuovi tributi e ulteriori incentivi, (in:) U. Ruffolo (ed.), Intelligenza artificiale. Il diritto, i diritti, l'etica, Milan 2020.

Uricchio A., Prospettive per l'introduzione di nuovi modelli di prelievo in materia di intelligenza artificiale anche alla luce del recovery plan, (in:) U. Ruffolo (ed.), XXVI Lezioni di Diritto dell'Intelligenza Artificiale, Turin 2021.

Uricchio A.F., Percorsi di diritto tributario, Bari 2017.

Uricchio A.F., Manuale di diritto tributario, Bari 2020.

Uricchio A.F., Prefazione, (in:) A.F. Uricchio, G. Riccio and U. Ruffolo (ed.), Intelligenza Artificiale tra etica e diritti. Prime riflessioni a seguito del libro bianco dell'Unione europea, Bari 2020.

Uricchio A.F., La sfida della strategia europea dell'Intelligenza Artificiale tra regolazione e tassazione, (in:) A.F. Uricchio, G. Riccio and U. Ruffolo (ed.), Intelligenza Artificiale tra etica e diritti. Prime riflessioni a seguito del libro bianco dell'Unione europea, Bari 2020.

Vacchi A., L'intelligenza artificiale nella produzione industriale: le ricadute sul mondo del lavoro, (in:) U. Ruffolo (ed.), XXVI Lezioni di Diritto dell'Intelligenza Artificiale, Turin 2021.

Walker J., Robot Tax. A Summary of Arguments 'For' and 'Against', 2 February 2017, https://emerj.com/ai-sector-overviews/robot-tax-summary-arguments/.

Wein L.E., The responsibility of intelligent artifacts: toward an automation jurisprudence, "Harvard Journal of Law & Technology" 1992, no. 6.

Wiener N., The human use of human beings. Cybernetics and society, Boston 1950.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.08

Received: 30.04.2021
Accepted: 30.07.2021

Wioleta Hryniewicka-Filipkowska
University of Białystok, Poland
w.hryniewicka@uwb.edu.pl
ORCID ID: https://orcid.org/0000–0003-2830–0796

Pros and Cons of Digital Solutions for the Implementation of Freedom of Movement and Residence in the Schengen Area in the Era of the COVID-19 Pandemic

Abstract: The COVID-19 pandemic caused by the SARS-CoV–2 coronavirus, which emerged in Europe in January 2020, gave rise to restrictions by European Union Member States on freedom of movement and residence in the Schengen area. Individual actions by states mobilized the EU to take formal steps as well as to implement practical solutions to coordinate the efforts of all Member States. Digital solutions belong to the practical measures. Their implementation may bring potential benefits but is also associated with the possibility of potential risks. This article presents the basic assumptions of freedom of movement and residence in the Schengen area and their limitations by Member States justified by public health reasons. The characteristics of digital solutions for facilitating freedom of movement during the COVID-19 pandemic are then presented, taking into account their effectiveness. The paper concludes with a presentation of the benefits and potential risks associated with the implementation of selected digital solutions by the European Union.
Keywords: COVID-19, free movement, public health, Schengen area

Introduction

Freedom of movement and residence within the Schengen area is considered to be one of the greatest achievements of European integration and the right most appreciated by EU citizens.[1] Millions of Europeans and third-country nationals use

1 P. Buras, Europe's Fragile Freedoms Facing a Coronavirus Stress Test, "Stiftung Genshagen Paper Series: Acting European? The European Union and the Weimar Triangle in the Coronavirus

it every year to travel for tourism, business or other purposes. These journeys are not subject to identity checks or conditions of entry and stay. However, there are situations when the long-forgotten physical borders between countries and the associated border controls must return for a while, thereby limiting the possibility of exercising this freedom, which is in accordance with European Union law. COVID-19 and its aftermath has verified the EU's capabilities and concepts in this regard.

The aim of this article is to discuss the restrictions on freedom of movement and residence in the Schengen area in relation to the protection of public health and to identify modern digital solutions to improve the implementation of freedom of movement in the era of the COVID-19 pandemic. The article adopts the following research hypothesis: not all tools introduced by the EU are effective and bring tangible benefits. Digital solutions carry potential risks.

The article was written using dogmatic and descriptive methods. The first was used to identify and interpret the provisions of EU law regulating restrictions on freedom of movement and residence in the Schengen area justified on public health grounds. The descriptive method was used to depict the digital solutions designed to implement freedom of movement and residence in the Schengen area in the era of the COVID-19 pandemic.

1. Restrictions on Freedom of Movement and Residence in the Schengen Area Justified on Public Health Grounds

Freedom of movement and residence within the territories of the Member States does not operate unconditionally. Under the law of the European Union, it is subject to certain limitations. In the preamble to the Treaty on European Union (hereinafter TEU), the Member States, while expressing their intention to facilitate the free movement of persons, stipulated that this freedom is to be exercised with due regard for the security of the nationals of the Member States by establishing an area of freedom, security and justice in accordance with the provisions of the treaties.[2] Subsequently, in the substantive provisions of the TEU, in Article 3(2), the EU legislator indicates that the free movement of persons operates in conjunction with the application of certain instruments for the control of the EU's external borders, asylum, immigration, and the prevention and combating of crime.[3] On the other hand, in Article 21(1) of the Treaty on the Functioning of the European Union (hereinafter

Crisis" 2020, no. 6, p. 2, http://www.stiftung-genshagen.de/uploads/media/Acting_ European_ No_6.pdf (accessed 20.04.2021).

2 Preamble of the TEU (Journal of Laws UE C 326 of 26.10.2012).

3 See T. Dubowski, Granica polsko-rosyjska jako zewnętrzna granica Unii Europejskiej, 'Białostockie Studia Prawnicze' 2011, no. 9, p. 78 and Art. 3(2) TEU (Journal of Laws UE C 326 of 26.10.2012).

TFEU), the EU legislator stresses that freedom of movement and residence within the territories of the Member States is to take into account the limitations and conditions laid down in the treaties and in the measures adopted to give them effect.[4] As Paweł Szewczyk rightly observes, the treaties do not explicitly specify which provisions should be taken into account in this case.[5] The right approach seems to be to adopt the limitations indicated for the broadly defined freedom of movement of persons, of which freedom of movement and residence within the territories of the Member States is a component. Those restrictions include grounds of public policy, public security and public health.[6] Moreover, conditions concerning restrictions on the exercising of the right to move and reside freely within the territory of the Member States may be laid down by secondary legislation. The restrictions on freedom of movement and residence caused by a threat to public health are supplemented by Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States; however, in terms of the occurrence of threats to public health, the regulations are quite sparing. Pursuant to it, Member States have the right to restrict freedom of movement and residence on the grounds of a threat to public health.[7] This is justified by the threat of epidemic diseases listed by the World Health Organization and the threat of other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions for nationals of the host Member State. In addition, under the Directive, Member States may require a person with the right of movement and residence to undergo, free of charge, a medical examination within three months of arrival in order to certify that he or she does not suffer from any epidemic or contagious disease. However, the Directive stipulates that such examinations must not be carried out routinely. The requirement to carry out such examinations is to be based on legitimate grounds.[8] When introducing restrictions due to the above premises, the state cannot justify them with economic objectives, e.g. to protect the domestic labour market. It seems that according to the principle of necessary requirements[9] indicated by the Court of

4 Art. 21(1) TFEU (Journal of Laws UE C 326 of 26.10.2012).

5 P. Szewczyk, Ograniczenia swobody przemieszczania się i pobytu obywateli UE uzasadnione względami porządku oraz bezpieczeństwa publicznego, 'Studia Prawnicze. Rozprawy i Materiały' 2016, vol. 19, no. 2, p. 187.

6 Art. 45(3) and Art. 52(1) TFEU (Journal of Laws UE C 326 of 26.10.2012).

7 Art. 27(1), Directive 2004/38 / EC.

8 *Ibidem*, Art. 29.

9 This principle applies directly to restrictions on the free movement of goods justified on valid grounds other than those set out in the Treaty. According to doctrinal considerations, it may apply in other cases, e.g. with regard to freedom of movement and residence. See M. Wiącek, Ograniczenia swobody przepływu osób w Unii Europejskiej – przypadek Romów we Francji w 2010 r., (in:) A. Frąckowiak-Adamska and A. Śledzińska-Simon (eds.), Sytuacja prawna i społeczna Romów w Europie, Wrocław 2011, pp. 56–57.

Justice of the European Union (CJEU) in the Cassis de Dijon case,[10] a Member State, when imposing restrictions on the exercising of freedom of movement and residence, including on the grounds of a threat to public health, must take measures which are proportionate, non-discriminatory and necessary to protect the public interest, but which take account of the EU's interest in exercising that freedom. The burden of proof for compliance with those requirements lies with the Member State.[11]

Until March 2020, the EU was only known to restrict freedom of movement and residence due to a need to ensure public order and security within the territory of Member States. For example, in recent years, Austria, Germany, France, Denmark, Sweden and Norway have maintained controls at the internal borders of the Schengen area in connection with the ongoing migration crisis in 2015–2016. Although the situation has improved significantly, these countries continue to maintain control at certain sections of the border, citing security concerns and terrorist threats.[12] We also witnessed the temporary closure of borders by France in 2015 due to a series of terrorist attacks, and the introduction of temporary controls at the internal borders of EU Member States in connection with the organization of political summits such as the G8, G20 or NATO and the organization of sports events such as Euro 2008 and Euro 2012.[13]

The COVID-19 pandemic is an unprecedented case of such a large-scale restriction on freedom of movement and residence in the Schengen area due to the premise of a public health threat in EU Member States. The first infection in Europe was reported on 24 January 2020 in France. Two months later, the European Union became the global epicentre of the disease, with a huge wave of cases first in Italy and then in Spain, France, the United Kingdom and the Benelux countries. By April 2020, the virus was present throughout Europe. The Member States of the Schengen zone, due to their right to restrict freedom in a public health emergency, individually began to implement restrictions. Various forms of controls were introduced at the internal borders of the Schengen zone. The restrictions consisted of reopening fewer border crossings; sanitary controls at border crossings, where travellers had to take their body temperature and fill in a card with their contact details and whereabouts

10 Judgment of the Court of 20 February 1979 in the case of Rewe-Zentral AG v. Bundesmonopolverwaltung für Branntwein. Reference for preliminary ruling: Hessisches Finanzgericht, C 120/78, p. 662.

11 Communication from the Commission, Guidelines concerning the exercise of the free movement of workers during COVID-19 outbreak 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3 A52020XC0330%2803%29 (accessed 20.04.2021).

12 J. Szymańska, Strefa Schengen w dobie pandemii Covid 19, 'Biuletyn Polski Instytut Spraw międzynarodowych' 2020, no. 62 (1994), pp.1–2.

13 See P. Rosik, T. Komornicki, S. Goliszek and P. Duma, Dostępność potencjałowa regionów w Europie – zasięg przestrzenny, długość podróży efekt granicy (EU-ROAD-ACC), Warsaw 2020, p. 31.

in order to be informed quickly if they came into contact with an infected person; travellers having to show a negative coronavirus test certificate; being banned from entering a Member State; and finally, closing all borders and having to undergo quarantine for several days after entering a Member State.[14]

In view of the situation, the measures taken by the states appeared to be justified, but the problem was that each of them basically acted individually, with different preventive measures. The manner in which they were introduced highlighted serious problems in the management of the Schengen area that had not previously been apparent. The restrictions that were introduced helped in the fight against the pandemic, but were imposed in an uncoordinated manner that affected even essential travel and the free movement of goods.[15]

It can be said that there was no uniform approach to the introduction of restrictions, which led to chaos, mutual tensions and, importantly, to the suspension by Member States of freedom of movement within the Schengen area. The problem was not just the various restrictions that were introduced, but the rapid pace of their implementation and modification. People travelling within the Schengen area lost track of the constantly changing rules and principles for crossing borders and staying in the Member States. Cross-border workers who live and work in two EU Member States were in an extremely difficult situation. People from the Polish-Czech or Polish-German border region had to face this kind of problem. The introduction of border controls made it very difficult for cross-border workers to move from their place of residence to their place of work and, if the borders were closed, forced them to choose between losing their earning opportunities and being separated from their families. Another problem was the obligation to undergo quarantine for several days after crossing the border or the obligation to perform regular coronavirus tests, which in turn entailed expense, limited availability and long waiting times for results.[16] The European Commission reacted to the above problem by issuing guidelines on the free movement of workers during the COVID-19 epidemic as early as 30 March 2020, paying particular attention to cross-border workers.[17] The proportionality of protection measures taken by Member States can also be questioned. For example, Hungary and Poland closed their borders to third-country nationals in March 2020 during the first wave of the pandemic in Europe.[18]

14 *Ibidem*, p. 32 and J. Szymańska, Strefa Schengen, *op. cit.*, pp. 1–2.

15 D. Schade, Crisis-Proof Schengen and Freedom of Movement: Lessons from the Covid-19 Pandemic, Hertie School, Jacques Delors Centre, Berlin 2021, p. 2.

16 See Polish cross-border workers stage protests against restrictions, 25 April 2020, https://www.thefirstnews.com/article/polish-cross-border-workers-stage-protests-against-restrictions-12252 (accessed 20.04.2021).

17 Communication from the Commission, Guidelines concerning, *op. cit.*

18 See S. Robin-Olivier, Free Movement of Workers in the Light of the COVID-19 Sanitary Crisis: From Restrictive Selection to Selective Mobility, 'European Papers' 2020, vol. 5, no. 1, p. 615.

The problem of the application of various measures by Member States to limit the spread of the pandemic was recognized by the European Union from the very beginning. The need to coordinate them was taken for granted, but in many cases this proved impossible, despite the best efforts of the European Commission and the support of other entities.[19] The organization has adopted a number of formal measures to coordinate its activities. At the EU level, a number of conclusions, recommendations, guidelines and communications have been developed to support the coordination efforts of the Member States and to guarantee freedom of movement within the Schengen area.[20] The EU has also decided to implement several digital solutions to help gradually restore freedom of movement and residence for EU Member States.

2. Selected Digital Solutions for the Implementation of Freedom of Movement of People in the Schengen Area During the COVID-19 Pandemic

The rapid spread of the virus required the EU institutions to take practical steps to slow down its transmission and protect the health and lives of EU citizens while allowing, as much as possible, the movement of people, goods and services in full compliance with health requirements. As a first step, the Re-open portal was launched on 15 June 2020, accessible on PC and mobile devices (since 14 December 2020, the portal is also available as a mobile application). The tool helps travellers and tourists

19 D. Schade, Crisis-Proof Schengen, *op. cit*., p. 2.

20 See Commission Guidelines for border management measures to protect health and ensure the availability of goods and essential services (OJ C 86I, 16.03.2020, p. 1); Commission Guidelines concerning the exercise of the free movement of workers during COVID-19 outbreak (OJ C 102I, 30.03.2020, p.12); 'Joint European Roadmap towards lifting COVID-19 containment measures' of the President of the European Commission and the President of the European Council, Commission Guidance on free movement of health professionals and minimum harmonisation of training in relation to COVID-19 emergency measures (OJ C 156, 08.05.2020, p. 1); Commission Communication towards a phased and coordinated approach for restoring freedom of movement and lifting internal border controls (OJ C 169, 15.05.2020, p. 30); Commission Communication on the third assessment of the application of the temporary restriction on non-essential travel to the EU (COM(2020) 299 final); Commission Guidelines on seasonal workers in the EU in the context of the COVID-19 outbreak (OJ C 235I, 17.07.2020, p. 1); Commission Communication on the implementation of the Green Lanes under the Guidelines for border management measures to protect health and ensure the availability of goods and essential services (OJ C 96I, 24.03.2020, p. 1); Commission Guidelines on Facilitating Air Cargo Operations during COVID-19 outbreak (OJ C 100I, 27.03.2020, p. 1); Commission Guidelines on protection of health, repatriation and travel arrangements for seafarers, passengers and other persons on board ships (OJ C 119, 14.04.2020, p.1); and Council Recommendation (EU) 2020/1475 of 13 October 2020 on a coordinated approach to the restriction of free movement in response to the COVID-19 pandemic (OJ L 337, 14.10.2020, pp. 3–9).

to travel safely within the Union in accordance with the applicable health regulations. The portal provides the basic and most up-to-date information on safety, travel, crossing internal borders, quarantine and testing for coronavirus in each Member State, Iceland, Liechtenstein, Norway and Switzerland. The information on the portal is pre-screened by the European Centre for Disease Prevention and Control and the Member States, and published in the 24 official languages of the EU.[21]

Other digital solutions being implemented to support coronavirus containment and thereby enable people's freedom of movement for work and tourism, in parallel with the Re-open portal, are national contact-tracing and alerting apps. The mechanism of an app is its installation on a smartphone device. Once it is launched, the app uses Bluetooth-based physical proximity data to detect other devices equipped with the same app in the vicinity. A person on the app who tests positive for COVID-19 alerts other app users that they have been within 2 metres of an infected person for a minimum of 15 minutes. At that point, those at risk of becoming infected can take necessary steps such as self-isolation and coronavirus testing to break the chain of infection. To integrate national contact-tracing and alerting apps, the European Commission has created an EU-wide system to ensure interoperability - the so-called 'network gateway'. The implementation of this solution allows the users to move around the European Union with a single app.

On 17 March 2021 the European Commission proposed the implementation of a new digital solution in the EU area, the Digital Green Certificate (also known as the COVID Certificate or Green Certificate), which in the era of the ongoing pandemic is expected to facilitate movement and stays in the Member States. The project will be fully implemented on 1 July 2021, and France is expected to be the first country to test the Digital COVID-19 Travel Certificate through the application.[22] The certificate is to be issued free of charge on paper or digitally, in English or in the official language of the issuing Member State. The document will be issued at the request of the person concerned by national treatment providers, e.g. primary care providers or vaccination centres. Each citizen will also be able to download the certificate personally from a selected national application (including a mobile device) dedicated to civic affairs or health issues (e.g. in Poland, the Internet Patient Account (IKP) and the mObywatel app). An individual will be able to obtain one of three types of certificate. Each of them will contain the date of issue; data confirming the identity of the person, including their name, surname and date of birth; a QR code; information on the certificate issuer; and a unique certificate identifier. The

21 Official website of the European Commission, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic_pl (accessed 25.04.2021).

22 France Becomes First EU Country to Start Testing Digital COVID-19 Travel Certificate Through App, 21 April 2021, https://www.schengenvisainfo.com/news/france-becomes-first-eu-country-to-start-testing-digital-covid-19-travel-certificate-through-app/ (accessed 02.06.2021).

first of these types of certificate is the vaccine receipt certificate, which, in addition to the above data, indicates the name of the disease to which the vaccination applies; the name of the vaccine received; the name of its manufacturer and the serial numbers of the dose(s); the date the vaccination was received; and the name of the country in which the vaccination was administered. This certificate is valid for one year. The certificate will not be available until 14 days after receiving a single dose or the second dose of a vaccine. The second type is the SARS-CoV–2 coronavirus negative test certificate, which includes information about the test performed (the type of test, name of test, name of test manufacturer), the date and time the sample was collected for testing, information about the place that performed the test, the test result and an indication of the country where the test was performed. This type of certificate is valid for 48 hours. At this stage, PCR tests are recognized. The last type of certificate is the COVID-19 recovery certificate, which indicates the date of a first positive test result and the name of the country where the test was performed. Recovery status is obtained 11 days after the test and is valid for 180 days. These types of certificates are not travel documents and do not replace the current requirement for travel documents in the form of an ID card or passport. Their possession exempts individuals from quarantine or the obligation to undergo additional tests. On the other hand, the absence of such a document when crossing a border will result in an obligation to fully comply with the prevailing pandemic restrictions. The certificates will be recognized by all Member States, as well as Iceland, Norway and Liechtenstein, and will be readable through a specially designed EU COVID Certificate System to which countries will subscribe. The certificate will be presented to the border authorities when travelling. By scanning the QR code on the certificate using the EU COVID Certificate app, the officer will read the identity of the certificate holder and check its authenticity and validity.[23]

The digital solutions proposed by the European Union to enable freedom of movement and residence in the Schengen area have been accepted by EU Member States. Their implementation gives hope for a quick return to pre-pandemic times. However, apart from the benefits that seem to be obvious, they carry potential threats.

23 Official website of the European Commission, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en; Paszport covidowy w aplikacji mObywatel. Od wakacji łatwiej będzie podróżować po UE, 21 May 2021, https://www.telepolis.pl/wiadomosci/aplikacje/ mobywatel-paszport-covidowy-podroze-po-ue-wakacje-2021 (accessed 20.05.2021).

3. Benefits of Implementing Selected Digital Solutions

Europeans find the Re-open portal useful for people who need to move to and stay in other Member States.[24] The successive waves of infections have shown how difficult it is to move around Europe when each country imposes its own sanitary restrictions. New information is constantly appearing in the media and on social networks, which becomes outdated quite quickly. The implementation of the tool provides the latest data on the epidemiological situation in individual countries and the rules of crossing internal EU borders. It seems that, despite the introduction of the Digital Green Certificate, portal will continue to fulfill its role. As statistics show, a large number of Europeans have not yet been vaccinated.[25] Among this social group, some people will choose never to receive the vaccine due to health aspects or their own beliefs. When travelling within the Schengen area, they will need to be aware of the current epidemiological situation in the countries. The portal is administered by the EU, which further strengthens the credibility and timeliness of its content. However, the content is not exhaustive, but it is important that it contains links to more detailed information. A definite disadvantage in the assessment of this tool is the minimum standard of accessibility for people with disabilities. The functioning of the portal does not entail serious risks; it can only make travelling difficult if the data is not up to date. However, so far, the data is supplemented on an ongoing basis.

Epidemic monitoring, which aims to limit the spread of the virus, mainly uses traditional contact-tracing methods. These involve identifying people who may have had contact with an infected person and providing information about the potential for infection, the need to undertake self-isolation and the provision of necessary care.[26] The idea of implementing contact-tracing and alerting apps also seemed to be a useful solution to complement the traditional methods mentioned. A definite benefit of this type of solution, highlighted by the Council of Europe, is the speed of transmission of information about the potential possibility of infection;[27] in the case of the spread of the virus, its new and more infectious variants are of great importance. Applications for contact tracing and alerting can be considered a tool to support the work of national sanitary services (using traditional methods of contact tracing). In Poland, especially during the second wave of infections, these services were becoming less and less efficient in quickly providing information to people

24 Chaos na wewnętrznych granicach, Witryna internetowa Filary Biznesu, 4 November 2020, , https://filarybiznesu.pl/chaos-na-wewnetrznych-granicach-ue/a6909 (accessed 25.04.2010).

25 Szczepienia przeciwko koronawirusowi w Polsce, Europie i na świecie – Zestawienie, https://www.euractiv.pl/section/zdrowie/news/pandemia-szczepienia-koronawirus-polska-europa-swiat-covid19-porownanie/ (accessed 25.04.2021).

26 Council of Europe, Digital solutions to fight Covid 19: 2020 Data protection report, October 2020, p. 25.

27 *Ibidem.*

who could potentially be infected. The application is a faster alternative tool to the information from the appropriate services to warn about the potential threat.

Another benefit of the solution is its reach. The national application works not only within the Member State, but thanks to the network gateway created by the European Commission, it enables the exchange of information between applications of other EU Member States. Therefore it can be useful when travelling and staying in other Member States that have adopted this solution. The benefits of the app were highlighted by Internal Market Commissioner Thierry Breton and Commissioner for Health and Food Safety Stella Kyriakides, among others. The latter stated that 'At a time when we are relaunching social and economic life, digital technologies are very useful to alert our citizens to the risk of infection, and to break the chains of infection.'[28] She also pointed out a crucial aspect of the success of the adopted solution, namely the number of users. In order for the app to fulfill its function, it must be used by approximately 60% of the population.[29] Despite positive opinions about the importance and benefits of this solution, it did not gain complete acceptance among EU Member States. The apps have been implemented in 22 countries, including 17 countries opting for decentralized architecture[30] (Austria, Belgium, Croatia, Czech Republic, Denmark, Estonia, Finland, Germany, Ireland, Italy, Latvia, Malta, Netherlands, Poland, Portugal, Slovenia, Spain) and five states in a centralized architecture[31] (Bulgaria, Cyprus, France, Slovakia, Hungary). However, five countries have decided not to implement this type of solution (Greece, Luxembourg, Lithuania, Romania, Sweden).[32]

Apps have not gained recognition among Europeans, as illustrated by publicly available data. In Germany, for example, the Corona-Warn-App (as of May 2021) had been downloaded by over 33% of citizens (28 million people),[33] which should be considered a good result in comparison with Poland, where the STOP COVID ProteGo Safe app (as of April 2021) was downloaded by fewer than 5% of citizens

28 European Commission Press Release, Coronavirus: Member States agree on an interoperability solution for mobile tracing and warning apps, Brussels, 16 June 2020, p. 1.

29 K. Szymielewicz, A. Obem and T. Zieliński, Jak Polska walczy z koronawirusem i dlaczego aplikacja nas przed nim nie ochroni?, https://panoptykon.org/protego-safe-ryzyka (accessed 20.05.2021).

30 This provides only for the processing of anonymous identifiers and the exchange of data, without involving the administration.

31 This enables the collection of data allowing for the unambiguous identification of individuals and the transfer of this data to the relevant administrative authorities (e.g. the sanitary administration, but also the police).

32 Council of Europe, Digital solutions, *op. cit.*, pp. 27–28.

33 Anzahl der Downloads der Corona-Warn-App über den Apple App Store und den Google Play Store in Deutschland von Juni 2020 bis Mai 2021, https://de.statista.com/statistik/daten/studie/1125951/umfrage/ downloads-der-corona-warn-app/ (accessed 03.06.2021).

(1.9 million).[34] It is difficult to estimate how many people in Europe currently use the app. Installing an app is not equivalent to using it and responding to warnings. The reasons for the low popularity of the use of apps will be discussed in the next part of the article devoted to threats resulting from digital solutions.

In the case of the Digital Green Certificate project, the Member States were initially very sceptical about the idea, which also caused uncertainty among Europeans, but in fact it is already a known solution and, in addition, is compliant with the law. For many years a similar tool has been used without which one cannot enter several countries in the world: the International Vaccination Booklet (the so-called yellow booklet). It is used to document vaccination against yellow fever, which, according to WHO health regulations, is a mandatory vaccination required for entry into parts of African and South American countries. The booklet is now an official document recognized around the world, and is obtained at the point where the vaccination is performed. Recommended vaccinations can also be recorded in this document.[35]

The benefits of implementing the Digital Green Certificate are obvious. The certificates will make the rules for crossing internal borders of the Schengen area uniform in all Member States, which is definitely a great convenience for travellers in Europe. Although border controls will not disappear, it can be predicted that the verification of travellers on the basis of the certificate will significantly streamline border traffic and thus reduce the waiting time to cross the border. What is more, the possibility of travelling for tourist purposes will return, which will bring measurable economic benefits, especially for countries whose main industry is tourism. Moving and staying in other Member States and returning to one's own country will not require tests or a quarantine period of several days. Cross-border workers will not have problems with getting to work and returning home to their families.

It can also be predicted that the introduction of the certificate will change the attitude of those hesitant or sceptical about receiving the vaccine, especially those who are keen on travelling. Although it will be possible to travel without the certificate, not having it will be a kind of complication in achieving travel goals, which will perhaps change the decision.

34 Odpowiedź na interpelację nr 22103 w sprawie aplikacji STOP COVID, https://www.sejm.gov.pl/sejm9.nsf/ InterpelacjaTresc.xsp?key=C2KJDB, Warsaw, 28.04.2021 (accessed 28.05.2021).

35 P. Orlikowski, Paszport covidowy budzi kontrowersje, a 'żółta książeczka' istnieje od lat. Prawnik wyjaśnia, 7 March 2021, https://www.money.pl/gospodarka/paszport-covidowy-budzi-kontrowersje-a-zolta-ksiazeczka-istnieje-od-lat-prawnik-wyjasnia-6613836302682688a.html (accessed 28.05.2021).

4. Potential Risks of Selected Digital Solutions

Digital solutions adopted within the EU carry the risk of potential threats. The implementation of the Digital Green Certificate and applications to trace and alert from infectious contacts has not been free from individuals' concerns about violations of privacy rights.[36] As rightly noticed by Zygmunt Niewiadomski and Marek Zirk-Sadowski, the effects of digitization may be particularly severe for citizens, and one of the most serious threats is the far-reaching restriction of privacy. The authors emphasize that the greater the degree of public threat, the more often the public authority uses measures restricting the private sphere of the citizen. This is because digitization offers greater opportunities for action, also for those who pose a security risk, so there is never-ending action in this area.[37]

In the case of apps, it is worth quoting the statement of the Commissioner for Health and Food Safety, Kyriakides, who said that their operation would respect data security, fundamental rights and the protection of individual privacy. To this end, the European Commission has developed a set of rules that must be strictly applied before the apps are made available. According to these principles, the installation and use of apps should be voluntary. The scope of the data collected is minimal, necessary for the provision of the service and does not allow the identification of specific individuals. The data is protected by state-of-the-art technologies, including encryption. Moreover, the European Commission does not allow the use of such data to determine the location or track the movement of people. The apps should be created using Bluetooth technology and the data obtained through them cannot be stored for more than 14 days. The Commissioner further assures that the apps will be turned off once the pandemic is over. She also confirms that health data is sensitive and its processing must follow strict rules. She points out that the aggregated statistical data collected does not allow the identification of individuals but only serves the purpose of contact tracing, and therefore the General Data Protection Regulation does not apply to it.[38] The above position was confirmed by the Polish Ministry of Digitization,

36 See Aplikacja 'Kwarantanna domowa' budzi wątpliwości obywateli. Rzecznik pisze do premiera, 13 November 2020, https://www.rpo.gov.pl/pl/content/rpo-do-premiera-aplikacja-kwarantanna-domowa-budzi-watpliwosci (accessed 29.04.2021).

37 Z. Niewiadomski and M. Zirk-Sadowski, Prawo wobec wyzwań epoki cyfryzacji, (in:) J. Gajewski, W. Paprocki and J. Pieriegud (eds.), Cyfryzacja gospodarki i społeczeństwa szanse i wyzwania dla sektorów infrastrukturalnych, Gdańsk 2016, pp. 205–209.

38 Official website of the European Commission, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/how-tracing-and-warning-apps-can-help-during-pandemi.pl (accessed 26.04.2021) and Art. 9 Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 04.05.2016, pp. 1–88).

which assured that the information held on the devices is anonymous, encoded and stored in the phone only for a period of two weeks.[39]

However, these assurances did not encourage mass adoption of the app. The idea failed for several reasons. Firstly, the EU Member States did not agree on a single path for implementing the app. They did not adopt a unified digital architecture and some states decided not to implement the tool, which definitely hindered interoperability. Moreover, not all countries that declared implementation of the project have registered in the common system. Secondly, it seems that the main reason for shying away from this solution by the majority of the public is a fear for the security and privacy of users and the fear of intervention by the sanitary administration and quarantine obligations. Moreover, digital experts point out that the application may report numerous false alarms, due to the fact that the Bluetooth signal reaches through walls. This means that the devices are communicating while their users are not actually in contact with each other. Therefore false messages may appear, which will needlessly limit the freedom of individuals. It should also be emphasized that the implementation of this type of solution may suppress the vigilance of citizens and lead to disregard for the main recommendations in terms of maintaining social distance and hygiene rules or limiting social contacts.[40]

As Alessandra Spadaro rightly points out, epidemics are a threat not only to human health but also to human rights,[41] and in this situation all human rights are at stake.[42] Fernando Dias Simões points out that there is a deep connection between these two aspects, because under human rights law, states have a duty to protect public health by struggling to control a pandemic, but they also have a duty to protect other fundamental human rights. Measures taken by states such as forced quarantine or travel restrictions can violate the rights to bodily integrity, to privacy, to freedom from inhuman or degrading treatment, to freedom from discrimination and to freedom of movement.[43]

As has already been emphasized, the Digital Green Certificate project raised a lot of emotions in its initial stage because of the protection of human rights. There were some voices asking if the certificates are really safe and whether the solutions used will protect the privacy of individuals, or if they pose a threat of far-reaching

39 ProteGOSafe – pobierz, zainstaluj, przetestuj, 29.04.2020, https://www.gov.pl/web/cyfryzacja/protego-safe--pobierz-zainstaluj-przetestuj (accessed 26.04.2020).

40 ProteGOSafe: instalować czy nie?, 3 August 2021, https://panoptykon.org/czy-instalowac-protego-safe (accessed 27.04.2021).

41 A. Spadaro, Covid 19: Testing the Limits of Human Rights, 'European Journal of Risk Regulation' 2020, vol. 11, no. 2, pp. 317–318.

42 K. Bennoune, 'Lest We Should Sleep': COVID-19 and Human Rights, 'American Journal of International Law' 2020, vol. 114, no. 4, p. 666.

43 F.D. Simões, COVID-19 and International Freedom of Movement: A Stranded Human Right? Hong Kong 2021, p. 5.

surveillance by the authorities issuing the documents. The European Commission assures EU citizens that they can feel safe: the document will contain a limited amount of information, and will not be able to be stored in the target Member States. Neither is a central EU-level database for the collection and storage of the documents envisaged. Processing and accss will only be possible for selected entities, the list of which will be publicly available, allowing citizens to exercise their data protection rights under the General Data Protection Regulation. In addition, although the COVID certificate has security features confirming its authenticity, it cannot be ruled out that there will be attempts to counterfeit it. At this point, it is difficult to say how the project will be implemented in practice and whether the privacy of certificate holders will be violated. The project is only in the implementation phase, so the coming months will show whether it has fulfilled its role and whether assurances about its security were true.

The EU assures that the proposed digital solutions do not risk discrimination. As Cecilia Rodriguez rightly sees, the implementation of such a tool sounds interesting at first glance. However, after deeper reflection, the question arises as to whether its use will not divide society, deepen inequalities, increase social exclusion and discriminate against certain social groups.[44] Information in the package leaflets of vaccines licensed in the EU indicates that there is a group of people who should not be vaccinated or who should take precautions when it is given. These include people who are allergic to the active substance or any of the other ingredients of the vaccine; who have a problem with blood clotting or bruising or are taking blood-thinning medicines; whose immune system is not working properly; pregnant or breast-feeding women; and children.[45] There is also a group of people who do not want to be vaccinated, which is their right. Vaccination for COVID-19 is not currently mandatory. Even if such compulsion is introduced, some in the legal community argue that it will be incompatible with the right to human dignity; the introduction of compulsory vaccination stands in opposition to this right and the right to health protection or the prohibition on subjecting individuals to scientific experiments, including medical ones, without their free consent. There are views that advocate that, under the current circumstances, submitting to COVID-19 vaccination is participation in a medical experiment.[46]

44 C. Rodriguez, Covid-19 Passports and Travel: Free, Non-Discriminatory and 'Non-fakeable'?, 16 May 2021, https://www.forbes.com/sites/ceciliarodriguez/2021/05/16/covid-19-passports-and-travel-free-non-discriminatory-and-non-fakeable/?sh=2b8128e0581c (accessed 15.06.2021).

45 Who should and shouldn't get the COVID-19 vaccine?, https://yalehealth.yale.edu/yale-covid-19-vaccine-program/who-should-and-shouldnt-get-covid-19-vaccine (accessed 17.06.2021).

46 Czy można przymusić do szczepienia przeciwko COVID-19, 13 January 2021, https://www.rp.pl/Zdrowie/301129912-Czy-mozna-przymusic-do-szczepienia-przeciwko-COVID-19.html (accessed 17.06.2021).

The groups of people indicated above who wish to cross a border will have to use a certificate stating a negative result of a test for coronavirus. At the moment the tests performed on their own are paid for privately. Even if there is a formal decision on reimbursement, it will take a logistical effort for the tests to be performed whenever a trip needs to occur. These people will be able to move without a certificate but with the full knowledge that they will be complying with existing restrictions in Member States, including quarantine and testing. The EU must ensure that those who are not certified have free access to coronavirus testing. This is especially important for economically vulnerable groups who need free and quick access to tests.

A potential threat is also the question of whether, in a situation where the pandemic will persist for many years, the EU will not go a step further in the future and decide to extend the scope of the certificates, following the example of solutions introduced, for example, in Israel and the United States and as is already the case in some EU Member States such as Denmark, Germany or Hungary. In these countries, access to public places such as restaurants, theatres, cinemas, hotels, sports and recreation centres or participation in major cultural and sporting events is already based on them. If this happens, unvaccinated people may become second-class citizens who would be excluded from many areas of social life.

Conclusions

Freedom of movement and residence in the Schengen area is one of the most important achievements of the European Union. The 2018 Eurobarometer survey shows that 88% of respondents identify the Schengen area as one of the EU's main achievements, and nearly three out of four respondents believe that it is not worth participating in the EU without freedom of movement.[47] The absence of internal borders, and therefore of border controls, has for many years been part of the European reality, creating facilities for tourism, trade, provision of services, education and work. The outbreak of the pandemic made it clear that the European Union was not prepared for this type of threat, which essentially prevented the exercise of freedom due to individual, albeit legally permissible, restrictions introduced by Member States. The pandemic also highlighted previously unseen problems in Schengen governance that prompted the EU to discuss undertaking necessary reforms. It has also introduced formal and digital solutions to coordinate Member States' individual efforts to curb virus transmission and restore freedom of movement. The research hypotheses presented in the introduction of this article have been confirmed. So far, the implemented digital solutions which were proposed by the EU are paying dividends. The biggest is the Digital Green Certificate; the

47 D. Schade, Crisis-Proof Schengen, *op. cit*., p. 2.

implementation of the project is expected to ultimately result in the rapid opening of the internal borders of the Schengen area. Nevertheless, already today we can see potential threats resulting from the adopted digital solutions. These include threats related to human rights, such as the limitation of privacy, fear of surveillance by the authorities issuing documents, risk of discrimination, risk of division in society and exclusion of individuals from many areas of social life. Due to the fact that the project is in the preliminary stage of implementation, it is difficult at this point to predict all the negative effects resulting from it. A final assessment will be possible in a few months, when the project will come into force in all EU Member States.

REFERENCES

Anzahl der Downloads der Corona-Warn-App über den Apple App Store und den Google Play Store in Deutschland von Juni 2020 bis Mai 2021, https://de.statista.com/statistik/daten/studie/1125951/umfrage/downloads-der-corona-warn-app/.

Aplikacja „Kwarantanna domowa" budzi wątpliwości obywateli. Rzecznik pisze do premiera, 13 November 2020, https://www.rpo.gov.pl/pl/content/rpo-do-premiera-aplikacja-kwarantanna-domowa-budzi-watpliwosci.

Bennoune K., "Lest We Should Sleep": COVID-19 and Human Rights, "American Journal of International Law" 2020, vol. 114, no. 4.

Buras P., Europe's Fragile Freedoms Facing a Coronavirus Stress Test, 'Stiftung Genshagen Paper Series: Acting European? The European Union and the Weimar Triangle in the Coronavirus Crisis' 2020, no. 6, http://www.stiftung-genshagen.de/uploads/media/Acting_ European_No_6.pdf.

Chaos na wewnętrznych granicach, Witryna internetowa Filary Biznesu, 4 November 2020, https://filarybiznesu.pl/chaos-na-wewnetrznych-granicach-ue/a6909.

Council of Europe, Digital solutions to fight Covid 19: 2020 Data protection report, October 2020.

Czy można przymusić do szczepienia przeciwko COVID-19, 13 January 2021, https://www.rp.pl/Zdrowie/301129912-Czy-mozna-przymusic-do-szczepienia-przeciwko-COVID-19.html.

Dubowski T., Granica polsko-rosyjska jako zewnętrzna granica Unii Europejskiej, „Białostockie Studia Prawnicze" 2011, no. 9.

European Commission Press Release, Coronavirus: Member States agree on an interoperability solution for mobile tracing and warning apps, Brussels, 16 June 2020.

France Becomes First EU Country to Start Testing Digital COVID-19 Travel Certificate Through App, 21 April 2021, https://www.schengenvisainfo.com/news/france-becomes-first-eu-country-to-start-testing-digital-covid-19-travel-certificate-through-app/.

France Becomes First EU Country to Start Testing Digital COVID-19 Travel Certificate Through App, https://www.schengenvisainfo.com/news/france-becomes-first-eu-country-to-start-testing-digital-covid-19-travel-certificate-through-app/.

Niewiadomski Z. and Zirk-Sadowski M., Prawo wobec wyzwań epoki cyfryzacji, (in:) J. Gajewski, W. Paprocki and J. Pieriegud (eds.), Cyfryzacja gospodarki i społeczeństwa szanse i wyzwania dla sektorów infrastrukturalnych, Gdańsk 2016.

Odpowiedź na interpelację nr 22103 w sprawie aplikacji STOP COVID, https://www.sejm.gov.pl/sejm9.nsf/ InterpelacjaTresc.xsp?key=C2KJDB, Warsaw, 28.04.2021.

Official website of the European Commission, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic_pl.

Official website of the European Commission, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/how-tracing-and-warning-apps-can-help-during-pandemi.pl.

Official website of the European Commission, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en.

Orlikowski P., Paszport covidowy budzi kontrowersje, a 'żółta książeczka' istnieje od lat. Prawnik wyjaśnia, 7 March 2021, https://www.money.pl/gospodarka/paszport-covidowy-budzi-kontrowersje-a-zolta-ksiazeczka-istnieje-od-lat-prawnik-wyjasnia-6613836302682688a.html.

Paszport covidowy w aplikacji mObywatel. Od wakacji łatwiej będzie podróżować po UE, 21 May 2021, https://www.telepolis.pl/wiadomosci/aplikacje/ mobywatel-paszport-covidowy-podroze-po-ue-wakacje-2021.

Polish cross-border workers stage protests against restrictions, 25 April 2020, https://www.thefirstnews.com/article/polish-cross-border-workers-stage-protests-against-restrictions-12252.

ProteGOSafe – pobierz, zainstaluj, przetestuj, 29.04.2020, https://www.gov.pl/web/cyfryzacja/protego-safe--pobierz-zainstaluj-przetestuj.

ProteGOSafe: instalować czy nie?, 3 August 2021, https://panoptykon.org/czy-instalowac-protego-safe.

Robin-Olivier S., Free Movement of Workers in the Light of the COVID-19 Sanitary Crisis: From Restrictive Selection to Selective Mobility, "European Papers" 2020, vol. 5, no. 1.

Rodriguez C., Covid-19 Passports and Travel: Free, Non-Discriminatory and 'Non-fakeable'?, 16 May 2021, https://www.forbes.com/sites/ceciliarodriguez/2021/05/16/covid-19-passports-and-travel-free-non-discriminatory-and-non-fakeable/?sh=2b8128e0581c.

Rosik P., Komornicki T., Goliszek S., and Duma P., Dostępność potencjałowa regionów w Europie – zasięg przestrzenny, długość podróży efekt granicy (EU-ROAD-ACC), Warsaw 2020.

Schade D., Crisis-Proof Schengen and Freedom of Movement: Lessons from the Covid-19 Pandemic, Hertie School, Jacques Delors Centre, Berlin 2021.

Simões F.D., COVID-19 and International Freedom of Movement: A Stranded Human Right? Hong Kong 2021.

Spadaro A., Covid 19: Testing the Limits of Human Rights, "European Journal of Risk Regulation" 2020, vol. 11, no. 2.

Szczepienia przeciwko koronawirusowi w Polsce, Europie i na świecie – Zestawienie, https://www.euractiv.pl/section/zdrowie/news/pandemia-szczepienia-koronawirus-polska-europa-swiat-covid19-porownanie/.

Szewczyk P., Ograniczenia swobody przemieszczania się i pobytu obywateli UE uzasadnione względami porządku oraz bezpieczeństwa publicznego, „Studia Prawnicze. Rozprawy i Materiały" 2016, vol. 19, no. 2.

Szymańska J., Strefa Schengen w dobie pandemii Covid 19, „Biuletyn Polski Instytut Spraw międzynarodowych" 2020, no. 62 (1994).

Szymielewicz K., Obem O., and Zieliński T., Jak Polska walczy z koronawirusem i dlaczego aplikacja nas przed nim nie ochroni?, https://panoptykon.org/protego-safe-ryzyka.

Who should and shouldn't get the COVID-19 vaccine?, https://yalehealth.yale.edu/yale-covid-19-vaccine-program/who-should-and-shouldnt-get-covid-19-vaccine.

Wiącek M., Ograniczenia swobody przepływu osób w Unii Europejskiej – przypadek Romów we Francji w 2010 r., (in:) A. Frąckowiak-Adamska and A. Śledzińska-Simon (eds.), Sytuacja prawna i społeczna Romów w Europie, Wrocław 2011.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.09

Received: 10.01.2021
Accepted: 11.04.2021

Wojciech Filipkowski
University of Bialystok, Poland
w.filipkowski@uwb.edu.pl
ORCID ID: https://orcid.org/0000–0001-6248–0888

Lorenzo Picarella
University of Milan, Italy
lorenzo.picarella@unimi.it
ORCID ID: https://orcid.org/0000–0002-5281–3017

Criminalizing Cybercrimes: Italian and Polish Experiences

Abstract: The rapidly advancing development of technology has both positive and negative effects on society and its members. Moreover, legislation can be slow to catch up with reality. This also applies to any reaction of society to new forms of social deviance. There is typically a delay in the introduction of legislation which tries to give a legal framework to new technological developments. The authors have taken an exploratory approach, analysing changes in Italian and Polish penal law relating to cybercrime that have occurred in Italy and Poland so far. The timeline, pace, and scope of the processes of criminalization are presented for each country. Even though both legislators had and have the same goal, differences in the approach to achieving it are visible. The conclusions may lead to changes in the penal policies of both countries.
Keywords: cybercrime, Italy, penal law, penal policy, Poland

Introduction

The Council of Europe Convention on Cybercrime, which was drawn up in Budapest on 23 November 2001 (entering into force in 2004), is of key importance in the fight against cybercrime. It was the first, and currently remains the only, act of international criminal law directly regulating the issue. This Convention was an effort to address the challenges posed by the development of information technology at global, regional, and local levels. Despite more than 20 years having passed since

its adoption, there are still asymmetries between countries in the criminalization of behaviour related to computers and their networks. From a scientific point of view, it is worth exploring these dissimilarities, as they may contribute to the search for the best legislative solutions in this area.

The main objective of this study is to examine the legislative actions taken by Italian and Polish legislators in the field of the criminalization of behaviour related to the functioning of computers and their networks. We have chosen two European countries which are members of the European Union, whose legal systems grew out of Roman law, belonging to one legal family and which have also ratified the Budapest Convention. At the same time, these are two countries which developed technologically in different ways, mainly due to the fact that Poland was an Eastern bloc country behind the Iron Curtain. Technological innovations arrived with a delay, which was then quickly compensated for in the period of political transition from the early 1990s.

The main research problem addressed in the study is to examine how the processes of the criminalization of pathological behaviour related to computers and their networks in both countries have developed in terms of time, pace, and scope. The hypothesis is that despite the above-mentioned similarities or dissimilarities, we are dealing with different approaches. In order to verify this hypothesis, the following research methods were used: dogmatic in relation to the regulations of both countries, desk research on Italian and Polish legal literature, and historical analysis.

1. Technological Evolution and its Impact on Penal Law

Technological advances have been characterized by the spread of computers (and subsequently other similar devices) throughout society in the last three decades. This evolution can be summed up in the following steps:[1]

- the first automatic data-processing devices (computers) – around and after the Second World War;
- the steady increase in the computing power and memory of these devices[2];
- the miniaturization of devices and falling prices per unit (microprocessors, microcomputers) – from the 1970s;
- increasingly widespread use in the public and private sectors, the connection of computers to local and wide area networks, exchanging data or information

1 P. Grabosky, Electronic Crime, Upper Saddle River 2007, p. 5ff.

2 M. Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Katowice 2015, pp. 31ff.

and collecting it in databases (the development of telecommunications) – from the 1970s;[3]
- the emergence of mobile devices (from the 1970s) and wireless access to networks;[4]
- the commercialization of the Internet (broad public access to online services, i.e. via the web) and the progressive expansion of cyberspace (electronic mail, websites, search engines, instant messaging, social networks, forums, blogs) – in the mid-1990s;[5]
- the emergence of social deviance associated with access to the network (e.g. addiction to information, games, smartphones)[6] – at the beginning of the 21st century, as well as the phenomenon of the dark web (around 2009);[7]
- the concept of the internet of things (IoT):[8] devices connected to the network (of varying complexity, with their own computing power) can communicate with each other autonomously without human intervention – since 2008; they generate most of the traffic in networks.[9]

The list presented above is not strictly chronological since some of the elements occurred across a wide time frame and did not occur in all countries at the same pace. Another future milestone in technological development will be the spread of information technology (IT) solutions with a high degree of automation in the processes of acquiring and processing data and information, and consequently the implementation of artificial intelligence.

3 In 1957, the United States Department of Defense began the ARPA project, which was designed to create a unbreakable system for information exchange. Initially a military, and later an academic, network, ARPA (ARPANet) made their creators realize the development potential inherent in interconnected computers. The first two-way connection in ARPANet between computers took place in 1969. See M. Pudełko, Prawdziwa Historia Internetu, Piekary Śląskie 2013, p. 91.

4 M. Grzelak and K. Liedel, Bezpieczeństwo w cyberprzestrzeni: Zagrożenia i wyzwania dla Polski – zarys problemu, „Bezpieczeństwo Narodowe" 2012, no. 22, p. 125.

5 The Transmission Control Protocol/Internet Protocol (TCP/IP) was developed as early as the 1970s and 1980s, and contributed to the creation of a single and effective standard for the exchange of information; an e-mail program, the prototype of today's File Transfer Protocol (FTP); and the Domain Name System (DNS). The first Internet domain, symbolics.com, was registered as early as 1995 and WWW (World Wide Web) technology was created in 1989.

6 W.A. Kasprzak, Ślady cyfrowe. Studium prawno-kryminalistyczne, Warsaw 2015, p. 50.

7 V. Benjamin, S. Samtani and H. Chen, Conducting Large-Scale Analyses of Underground Hacker Communities, (in:) T.J. Holt (ed.), Cybercrime Through an Interdisciplinary Lens, Abingdon 2017, p. 62ff.

8 E.M. Kwiatkowska, Development of the Internet of Things: Opportunities and Threats, "Internet Kwartalnik Antymonopolowy i Regulacyjny" 2014, vol. 3, no. 8, p. 4.

9 2020 Global Networking Trends Report, CISCO, https://www.cisco.com/c/dam/m/en_us/solutions/enterprise-networks/networking-report/files/GLBL-ENG_NB-06_0_NA_RPT_PDF_MOFU-no-NetworkingTrendsReport-NB_rpten018612_5.pdf (accessed on 05.04.2021).

This technological evolution, and specifically the rise of cyberspace, has produced a change in the nature of human activities, criminal ones included. They now present new characteristics, including:[10]

- dematerialization (the resources/goods on the Internet do not possess physical components, but mainly consist in data and information);
- automation (technological progress has significantly reduced both the need for human intervention in IT operations and the minimum skill level needed to be competent in using IT);
- increased speed (the ever-increasing network speed has enhanced the pace of human activities);
- deterritorialization (the Internet is a space potentially limitless and without borders);
- ubiquity (computer users can carry out online activities from different virtual places at the same time);
- detemporalization (computer activities can be carried out without the direct intervention of the user by using automated software that will start operating at a specific time decided by the user themselves);
- overlapping between private and public dimensions (e.g the great amount of personal data uploaded to the web, especially to social networks).

These characteristics differ significantly from 'traditional' human physical activities, and they have inevitably made a significant impact on penal law, challenging its traditional principles and doctrines concerning:[11]

- the *actus reus*, the *mens rea*, and the nexus of causality (e.g. the act of the offender in cyberspace often loses importance in favour of the automated operations of software, because it is the latter which directly harms the victim; the role of the internet service provider is paradigmatic of these new challenges);
- the *locus commissi delicti* (considering that online activities are not subject to traditional borders, it may be challenging to determine the competent jurisdiction, e.g. in the case of international cyberattacks);
- harm and legally protected goods (e.g. the emergence of IT confidentiality and IT security as new potential legal goods that needs autonomous protection).

10 R. Flor, Lotta alla 'criminalità informatica' e tutela di 'tradizionali' e 'nuovi' diritti fondamentali nell'era di internet, 'Diritto penale contemporaneo' 20 September 2012; R. Flor, La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative, (in:) A. Cadoppi, S. Canestrari, A. Manna and M. Papa (eds.), Trattato di Diritto penale – Cybercrime, Milan 2019, p. 141ff.

11 L. Picotti, Diritto penale e tecnologie informatiche: una visione d'insieme, (in:) A. Cadoppi et al. (eds.), Trattato di Diritto penale, *op. cit.*, p. 34ff.

Even if most cybercrimes simply consist of a new way of committing traditional offences,[12] legislators have been forced to make changes in penal law through amendments or the introduction of new offences, because cybercrimes evade the scope of traditional offences due to the aforementioned characteristics.[13]

At the international level, the Council of Europe Convention on Cybercrime, which was drawn up in Budapest on 23 November 2001 (entering into force on 1 June 2004), was the first act of international penal law of the information-society era directly regulating the above matters, and is still the most influential.[14] The Convention, which aimed to harmonize substantial penal law and improve judicial cooperation between Member States, has greatly influenced national legislation on cybercrime, including that of Italy and Poland.

2. National Experiences

A. The Italian Penal Law System

In this section, we summarize the evolution of penal law legislation against cybercrime in Italy, highlighting its timeline and main features.[15] The first law that introduced a cybercrime offence in the Penal Code was enacted in 1978. In the following years, the legislator's activity was characterized by two systematic interventions, in 1993 and 2008, with the latter constituting the transposition of the Budapest Convention. Italian legislation against cybercrime has also been characterized by several narrow-scope interventions since the mid-1990s.

Regarding the criminalization of cybercrime behaviours, the legislation adopted two different approaches:[16]

1) the extension of the scope of 'traditional' offences, introducing new ways to commit the crime, or cyber goods as the target of the *actus reus*;
2) the creation of new offences.

12 P. Grabosky, Virtual Criminality: Old Wine in New Bottles? "Social & Legal Studies" 2001, no. 2, p. 243ff.

13 C. Pecorella, Reati informatici, (in:) Enciclopedia del diritto – annali, Milan 2017, p. 707ff.

14 For a specific analysis, see R. Flor, Cyber-criminality: le fonti internazionali ed europee, (in:) A. Cadoppi A. Cadoppi, S. Canestrari, A. Manna and M. Papa (eds.), Trattato di Diritto penale, *op. cit.*, p. 97ff. and A. Adamski, Przestępczość w cyberprzestrzeni. Prawne środki przeciw działania zjawisku w Polsce na tle projektu konwencji Rady Europy, Toruń 2001, p. 17.

15 Concerning the scope of the research, we take into consideration only 'cybercrimes and computer crimes *in a strict sense*' (for these definitions, see L. Picotti, Diritto penale, *op. cit.*, p. 77ff) or as covered by the Budapest Convention as far as the scope of criminalization is concerned. These definitions, which embody all the offences, make explicit reference to the computer or cyber dimension present in the Penal Code.

16 C. Pecorella, Reati informatici, *op. cit.*, p. 712ff.

In both cases, the new cybercrime offences were placed in the Penal Code next to their traditional counterparts, in that way avoiding the creation of an ad hoc section. This legislative choice was aimed at assimilating, as far as possible, the *ratio puniendi* and the structure of the old offences with the new ones.[17] Although this approach has been praised by the literature, it might lead to the transfer of the old offences' interpretation schemes to the new offences, increasing the risk of limiting their application.[18]

In general, the legislation has introduced and amended several offences to counter cybercrime through the years, trying to cover any possible gaps in the substantive penal law legislation. Even if the legislation's activity has mainly achieved its target, at the same time it has received a fair dose of criticism from the academic literature. The most recurrent issue that has been highlighted concerns the lack of technical accuracy in the creation of new offences or the amendment of 'old' ones, showing little attention to and/or knowledge of penal law and information and communications technology (ICT).[19] For example, the cyberfraud offence (Article 640-ter), due to the choice to distance it from the traditional fraud offence model, has not been a useful tool for prosecutors to counter cyberfraud; instead, its scope was more centred towards damage to computer systems and data.[20] The expansion of the definition of 'correspondence' in Article 616, without an explicit reference to the 'open' or 'closed' nature of it, has caused problems in the interpretation of the offence and has produced a loophole in the protection of the secrecy of correspondence, for example, in the case of the employer who reads the messages that employees receive on the company's e-mail accounts.[21] Article 392 does not make explicit reference to 'data' and 'programs' as possible objects of damage, therefore it has not been frequently applied in case law.[22] The element of 'belonging to another' in Article 635-bis (damage to computer data, information, or programs), which reflects the structure of the offence of vandalism on which Article 635-bis was based, makes it difficult to identify the victim of the crime, because data, information, and programs, due to their immaterial nature, cannot be owned or possessed in the same way as things.[23] It is also important to underline that there are very limited cases of damage to computer data and systems (Article 635 from -bis to -quinquies) in Italian jurisprudence.[24]

17 L. Picotti, Diritto penale, *op. cit.*, pp. 58–59.
18 *Ibidem*.
19 The legislator was only able to partially fix this general issue in 2008; L. Picotti, La ratifica della Convenzione Cybercrime del Consiglio d'Europa: Profili di diritto penale sostanziale, 'Diritto penale e processo' 2008, no. 6, p. 700ff.
20 C. Pecorella, Reati informatici, *op. cit.*, pp. 721–722.
21 *Ibidem*, p. 714.
22 *Ibidem*, p. 716.
23 L. Picotti, La ratifica della Convenzione Cybercrime, *op. cit.*, p. 711.
24 C. Pecorella, Reati informatici, *op. cit.*, p. 720.

Moreover, in some offences, particularly those concerning the actions that precede illegal access to a computer system (Article 615-quater and -quinquies), criminal liability is expanded to behaviours that are not harmful.[25] In other cases, specifically Article 635-ter and -quinquies, the offences are vague, and from their penalties and collocation in the Penal Code it is not clear which penal law policy the legislator has pursued.[26] (See Table 1.)

B. The Polish Penal Law System

There are three milestones in the history of Polish legislation regarding offences connected with computers or their networks – in 1997, 2004, and in 2017. Twelve types of behaviour were criminalized for the first time in the 1997 Polish Penal Code[27] (see Table 2). They included behaviours aimed not only against confidentiality, integrity, and availability of computer data, but also state interest, public safety, sexual freedom and decency, credibility of documents, and property. The introduction of computer offences to the penal code might be considered as a 'revolution' in the Polish penal law system in those times.

Table 1. The timetable of changes to the Italian Penal Code (IPC) regarding cybercrimes

Article of IPC	L. 191/78	L. 547/1993	L. 269/1998	L. 48/2008	L. 172/2012	D.L. 93/2013	D.L. 7/2015	D.LGS. 7/2016	L. 69/2019
270-quinquies, § 2[1]							C		
392, § 3[2]		E							
420[3]	N	A		AB					
491-bis[4]		N		A				A	
495-bis[5]				N					
600-ter[6]			N						
600-quater[7]			N						
600-undecies[8]					N				
612-bis, co. 2[9]						C			
612-ter[10]									N
615-ter[11]		N							
615-quater[12]		N							
615-quinquies[13]		N		A					
616, § 4[14]		E							
617-quater[15]		N							

25 *Ibidem*, p. 710.

26 *Ibidem*, p. 714ff.

27 This has been in force since 1 September 1998 (Official Journal of the Republic of Poland (OJ) 1997.88.553).

617-quinquies[16]		N							
617-sexies[17]		N							
621, § 2[18]		E							
635-bis[19]		N		A				A	
635-ter[20]				N				A	
635-quater[21]				N				A	
635-quinquies[22]				N				A	
640-ter[23]		N				A			
640-quinquies[24]				N					

Key: N (new offence); A (amended); C (new aggravating circumstance added to an existing offence); E (expanding the scope of a 'traditional' offence); AB (abolished).

Source: Authors' own study.

1. 'Training for terrorism-oriented activities', Offences against the State.
2. 'Arbitrary exercise of one's rights with violence to objects', Offences against justice.
3. 'Attack against public utility structures', Offences against public order.
4. 'Forgery of digital documents', Offences against public faith.
5. 'False communication of information about one's or another's identity of personal qualities to the certifier of digital signatures', Offences against public faith.
6. 'Child-abuse pornography', Offences against the person.
7. 'Disposal of child-abuse contents', Offences against the person.
8. 'Child grooming', Offences against the person.
9. 'Stalking', Offences against the person.
10. 'Revenge porn', Offences against the person.
11. 'Illegal access to a cyber system', Offences against the person.
12. 'Unlawful disposal or provision of access codes', Offences against the person.
13. 'Unlawful provision of malicious computer programs', Offences against the person.
14. 'Violation, theft and destruction of correspondence', Offences against the person.
15. 'Unlawful interception, obstruction or interruption of cyber communication', Offences against the person.
16. 'Installment of devices aimed at intercepting, obstructing or interrupting cyber communication', Offences against the person.
17. 'Falsification, forgery or destruction of cyber communication contents', Offences against the person.
18. 'Disclosure of secret documents' contents', Offences against the person.
19. 'Damage to computer information, data and programs', Offences against property.
20. 'Damage to computer information, data and programs used by the State or a public utility', Offences against property.
21. 'Damage to computer systems', Offences against property.
22. 'Damage to computer systems of a public utility', Offences against property.
23. 'Cyberfraud', Offences against property.
24. 'Cyberfraud committed by a person who gives electronic signature certification services', Offences against property.

This brief description indicates that the development of Polish computer criminal law has not evolved in line with the progress of technology and its dissemination worldwide. Polish legislation had to catch up relatively quickly in terms of its legal

penal response to manifestations of the pathological use of computers and, later on, networks. This is different from the Italian legislation described earlier, which has a much longer history in this respect.

For this reason, so far there are only cases of creating new types of offences or updating the descriptions of the constituent elements of an offence in the Polish Penal Code. These are described in Table 2 as N (new offences) or A (amended). There are no cases described above in relation to changes in Italian penal law, such as a new aggravating circumstance added to an existing offence, expanding the scope of a 'traditional' offence, or abolished offences.

More types of offences were then introduced to the Polish penal law system: two in 2004 and one in 2008. The second milestone was not only about introducing new types of offences; the changes introduced lead to the conclusion that criminalization went beyond computer offences to encompass the already-developing Internet and the pathological behaviours emerging along with it. The following examples of the 2004 amendments to the constituent elements of offences can be pointed out:

- 'entering a computer network' was changed to 'entering an information system';
- 'transmission of information' was changed to 'transmission of computer data';
- 'change of record' or 'change of information' was changed to 'computer data';
- 'transmission of information' was changed to 'transfer of computer data';
- 'recording on a computer storage medium' was changed to 'recording of computer data'.

There is an evident shift away from computers strictly as devices towards broadening the scope of criminalization to include behaviour related to their networks: local or wide area networks. This process has also affected the information entered, processed, and accessed in these systems This change in the constituent elements of the offences was intended to broaden the concept of computer data.. This trend was confirmed with the subsequent 2008 amendments. Attention was drawn to security breaches (also in the sense of software, not merely hardware) in telecommunications networks, and the computer storage medium was changed to a recording of computer data.

Table 2. The timetable of changes to the Polish Penal Code (PPC) regarding cybercrimes

Article of PPC	1998	2004[25]	2005	2008	2014	2017
130 § 3[26]	N	A				
165 § 1, item 4[27]	N	A				
202 § 3[28]	N	A	A		A	

267[29]	N			A		
268[30]	N			A		
268a[31]		N				
269[32]	N	A		A		
269a[33]		N				A
269b[34]		N				A
270 § 1[35]	N					
278 § 2[36]	N					
278 § 5[37]	N					
285 § 1[38]	N					
287[39]	N	A				
293[40]	N					

Key: N (new offence); A (amended).
Source: Authors' own study.

25. OJ 2004.69.626.
26. 'Computer espionage', Offences against the Republic of Poland.
27. 'Causing danger by interfering with, obstructing or otherwise affecting automatic processing, storage or transmission of computer data', Offences against public safety.
28. 'Production, recording or importing, storing or possessing with a view to distribution, or distribution or presentation of pornographic content with the participation of a minor, or pornographic content involving the display of violence or the use of an animal', Offences against sexual freedom and decency.
29. 'Obtaining information unlawfully', Offences against information protection.
30. 'Obstructing access to information', Offences against information protection.
31. 'Destruction of information in databases', Offences against information protection.
32. 'Damaging computer data of special importance to the country', Offences against information protection.
33. 'Interference with the operation of an IT or data communications system or network', Offences against information protection.
34. 'Unlawful production, acquisition, disposal or provision of malicious computer programs', Offences against information protection.
35. 'Forgery of digital documents', Offences against the credibility of documents.
36. 'Theft of a computer program', Offences against property.
37. 'Theft of an ATM card', Offences against property.
38. 'Telecommunication fraud', Offences against property.
39. 'Computer fraud', Offences against property.
40. 'Obtaining stolen software', Offences against property.

The most recent amendments, of 2017, are the separation of systems from 'computer' to 'IT' and 'ICT'. In the explanatory memorandum to this amendment, we can find the explicit statement that 'the term "computer system" does not correspond to modern IT or ICT reality and raises interpretation doubts'. However, the amendments introduced have led to more interpretation problems. The concepts of telecommunication networks and systems are semantically similar. Although they have not been defined in the Penal Code, this has been done in other laws. According to the principles of interpretation, the same meaning should be given to the concepts, especially since they are legal definitions in such legal acts as the Act of 2002 on the provision of electronic services,[28] the Act of 2005 on the computerization of the activities of entities performing public tasks,[29] and the Act of 2004 – Telecommunications Law.[30] This renders some articles unnecessary, for example Article 268(a) of the PPC, which falls within the scope of Article 269(a) of the PPC.[31]

There are two basic problems in the case of Polish penal regulations, and they both concern the issue of assigning meaning to the constituent elements of the offences. The first relates to their 'extension' to new behaviours. The second problem is the issue of ensuring the consistency of their meaning in the context of the entire Polish legal system.

3. Final notes

The changes relating to the adaptation of penal law to developing IT technologies started much earlier in Italy than in Poland. In the former case, the first intervention dated back to 1978, in the latter case to 1997. The gradual evolution of Italian legislation has gone in two directions: expanding the scope of 'traditional' offences and creating entirely new ones. The latter direction was the one that was taken up by Polish legislation. It has taken advantage of a new penal code to introduce completely new types of offence, instead of updating or amending the traditional ones. Another consequence is that the types of offences in Italian law are far more numerous and have a more dispersed and detailed character. In the case of Polish law, the offences related to cybercrime are fewer, and they have been constructed using descriptions

28 OJ 2020.344.

29 OJ 2020.346

30 OJ 2019.2460.

31 A. Lach, Komentarz do art. 269a (in:) V. Konarska-Wrzosek (ed.), Kodeks karny. Komentarz, wyd. III, Warsaw 2020 – https://sip.lex.pl/#/commentary/587715949/630826/konarska-wrzosek-violetta-red-kodeks-karny-komentarz-wyd-iii?cm=URELATIONS; W. Wróbel and D. Zając, Komentarz do art. 269a (in:), W. Wróbel and A. Zoll (eds.), Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. 212–277d, Warsaw 2017 – https://sip.lex.pl/#/commentary/587746553/543993/wrobel-wlodzimierz-red-zoll-andrzej-red-kodeks-karny-czesc-szczegolna-tom-ii-czesc-ii-komentarz...?cm=URELATIONS.

which are more general in semantical scope. Nevertheless, both legislative bodies have problems in adjusting the descriptions of offences to the ongoing IT revolution. This is an example of the common perception that the law has not kept up with technological progress, which criminals are attempting to abuse.

Considering the constant evolution of IT and the experience of these two countries in criminalizing cybercrime, in our opinion the legislative bodies should pay attention to some elements for future amendments to the law: firstly, it is necessary to better understand cyberspace and its nature; secondly, it would be useful to rethink some of the traditional categories of penal law in the light of the new technologies; finally, it would be wise to adopt a more international approach in order to harmonize different legislations and foster international cooperation.

REFERENCES

2020 Global Networking Trends Report, CISCO – https://www.cisco.com/c/dam/m/en_us/solutions/enterprise-networks/networking-report/files/GLBL-ENG_NB-06_0_NA_RPT_PDF_MOFU-no-NetworkingTrendsReport-NB_rpten018612_5.pdf.

Adamski A., Przestępczość w cyberprzestrzeni. Prawne środki przeciw działania zjawisku w Polsce na tle projektu konwencji Rady Europy, Toruń 2001.

Benjamin V., Samtani S. and Chen H., Conducting large-scale analyses of underground hacker communities, (in:) T.J. Holt (ed.), Cybercrime Through an Interdisciplinary Lens, Abingdon 2017.

Flor R., Cyber-criminality: le fonti internazionali ed europee, (in:) A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), Trattato di Diritto penale – Cybercrime, Milan 2019.

Flor R., La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative, (in:) A. Cadoppi, S. Canestrari, A. Manna and M. Papa (eds.), Trattato di Diritto penale – Cybercrime, Milan 2019.

Flor R., Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet, (in:) Diritto penale contemporaneo, 20 settembre 2012.

Grabosky P., Electronic crime, New Jersey 2007.

Grabosky P., Virtual Criminality: Old Wine in New Bottles? „Social & Legal Studies" 2001, no. 2.

Grzelak M. and Liedel K., Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, „Bezpieczeństwo Narodowe" 2012, no. 22.

Kasprzak W.A., Ślady cyfrowe. Studium prawno-kryminalistyczne, Warsaw 2015.

Kwiatkowska E.M., Development of the Internet of Things - opportunities and threats, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, vol. 3, no. 8.

Lach A., Komentarz do art. 269a, (in:) V. Konarska-Wrzosek (ed.), Kodeks karny. Komentarz, wyd. III, Warsaw 2020 – https://sip.lex.pl/#/commentary/587715949/630826/konarska-wrzosek-violetta-red-kodeks-karny-komentarz-wyd-iii?cm=URELATIONS.

Lakomy M., Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Katowice 2015.

Pecorella C., Reati informatici, (in:) Enciclopedia del diritto - annali, Milan 2017.

Picotti L., Diritto penale e tecnologie informatiche: una visione d'insieme, (in:) A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), Trattato di Diritto penale – Cybercrime, Milan 2019.

Picotti L., La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale, "Diritto penale e processo" 2008, no. 6.

Pudełko M., Prawdziwa Historia Internetu, Piekary Śląskie 2013.

Wróbel W. and Zając D., Komentarz do art. 269a, (in:), W. Wróbel and A. Zoll (eds.), Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. 212–277d, Warsaw 2017 – https://sip.lex.pl/#/commentary/587746553/543993/wrobel-wlodzimierz-red-zoll-andrzej-red-kodeks-karny-czesc-szczegolna-tom-ii-czesc-ii-komentarz...?cm=URELATIONS.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.10

Received: 27.03.2021
Accepted: 15.06.2021

Emil Kruk
Maria Curie-Sklodowska University, Poland
emil.kruk@umcs.pl
ORCID ID: https://orcid.org/0000–0002-7954–0303

Industrial Breeding of Animals: Legal and Ethical Issues[1]

Abstract: The main purpose of this article is to discuss the basic legal and axiological problems that are associated with technological advances in animal rearing and breeding. The implementation of this research task required, first and foremost, the definition of the concept of 'welfare' and the identification of basic legal provisions determining the welfare of livestock in Poland. Moreover, the article addresses the ethical aspect of the problems associated with the implementation of modern animal welfare technologies, including the role of Christianity in shaping moral attitudes in this area. The paper is also an attempt to define the level of public awareness about the need to protect animals and the perception of problems related to the intensification of livestock production. The need to address the issue stems, above all, from the fact that human life and our attitudes towards animals are changing with the development of civilization. In any event, the changes that have taken place in this area over the past decades make the problem topical and lead to a reflection on the welfare of animals kept in industrial farming conditions. It is assumed that the research carried out will contribute to the development of an optimal legal model for the protection of livestock. Even the mere dissemination of the results will raise public awareness of the humanitarian protection of animals, which is one of the preconditions for further progress in civilization.

Keywords: animals, breeding, industry, welfare, law, ethics

1 This publication was prepared within a research project entitled 'The Administrative Law Animal Protection Model' included in the application registered under number 2016/23/D/HS5/01820 in the Funding Stream Service system administered by the National Information Processing Institute, and accepted for financing within the competition announced by the National Science Centre, Poland, 'SONATA 12', on the basis of the decision made by the director of the National Science Centre in Krakow on 16 May 2017 (decision no. DEC-2016/23/D/HS5/01820, contract no. UMO-2016/23/D/HS5/01820).

Introductory Remarks

Most livestock is now kept under conditions of industrial rearing, which have developed intensively since the 1960s. This is largely a result of cooperation between the meat industry and scientists. This cooperation has covered not only the conditions for keeping these animals or the ways in which they are fed, but also genetic selection aimed at increasing their yield, which means greater and faster weight gain, greater milk or egg yield, etc.[2]Unfortunately, all this occurs at the expense of the quality of life of the animals, and generally it proves that technological progress does not always go hand in hand with moral progress –just the opposite. This is perfectly reflected in the words of Israeli historian Yuval Noah Harari, who believes that 'industrial farming is one of the worst crimes in history' and the fate of industrially bred animals is one of the most urgent ethical concerns of our time.[3] One cannot help but share this view, especially considering that the methods of industrial breeding are simply cruel, and animals in this process are treated as exploited resources or machines for processing cheap feed into the desired final product – egg, milk, meat, fur. This is the other side of progress that prompts us to address the issues pointed out in the title of this study. It should be noted that its main aim is to discuss the problems related to the humanitarian protection of farm animals, i.e. the protection motivated by ethical, non-economic considerations. The findings made in this regard will allow us to verify the hypothesis that the current model of livestock protection, being both a consequence and a manifestation of civilizational development, requires a thorough change in order to improve both animal welfare and the quality of human life. This will require clarifying the concept of 'welfare', discussing the basic legal and axiological problems related to technological progress in animal rearing and breeding, as well as determining the degree of social awareness of the problems related to the intensification of animal production. These issues will be further discussed in the order above.

2 According to the data provided by B. Grabowska, currently 99.9% of broilers, 97% of laying hens, 99% of turkeys, 95% of pigs and 78% of cattle are on industrial farms. As regards the intensification of industrial breeding, for example, between 1935 and 1995 the weight of the average broiler increased by 65%, while its lifetime decreased by 60% and its nutritional requirements decreased by 57%. The fact that these changes have an adverse effect on the welfare of livestock is demonstrated, inter alia, by the fact that they need to have medicines and vitamin supplements continuously administered. As many as 90% of broilers have visible bone disorders and 26% suffer from bone diseases causing chronic pain. See B. Grabowska, Zmiany relacji człowiek – zwierzę, czyli cena postępu, 'Kultura i Wartości' 2014, no. 2, pp. 111–112 and the literature cited therein.

3 Y.N. Harari, Industrial farming is one of the worst crimes in history, 'The Guardian' 25 September 2015, https://www.theguardian.com/books/2015/sep/25/industrial-farming-one-worst-crimes-history-ethical-question (accessed 19.04.2021).

1. Animal Welfare

There is no doubt that animal welfare[4] is one of the most important elements of sustainable development. Therefore, it is important to understand it properly. At this point, the opinion of the World Organisation for Animal Health (OIE) may be helpful, according to which, 'Animal welfare means the physical and mental state of an animal in relation to the conditions in which it lives and dies. An animal experiences good welfare if the animal is healthy, comfortable, well nourished, safe, is not suffering from unpleasant states such as pain, fear and distress, and is able to express behaviours that are important for its physical and mental state'.[5] The issue in question is therefore of a multidimensional nature, and a number of rules are required to ensure animal welfare in animal production systems. These primarily cover the use of appropriate genetic selection, which should take account of animal health and welfare; ensuring that animals have the right environmental conditions; providing animals with conditions to meet the needs typical of their species; adequate animal nutrition; ensuring that animals have sufficient space to move around freely; protecting animals from diseases and parasites; not putting animals at risk of unnecessary pain and stress; and animal handlers having the right qualifications.[6] It is even more important that improving the welfare of livestock can increase the production and safety of food and thus lead to economic benefits. However, the most important thing is to be aware that any use of animals entails ethical responsibility for ensuring their welfare as much as possible.

Unfortunately, as practice shows, many of the solutions used in mass animal breeding do not take the above-mentioned requirements into account. This is the case because industrial animal breeding is driven by one goal: to produce more and cheaper.[7] A simple consequence of this fact is a drastic deterioration in the welfare of livestock. It is sufficient to mention problems associated with the spatial concentration of large-scale farms and the crowding of animals bred for meat, milk,

4 'Animal welfare is a term that describes a potentially measurable quality of a living animal at a particular time and hence is a scientific concept.' See D.M. Broom, A History of Animal Welfare Science, "Acta Biotheoretica" 2011, no. 59, pp. 121–137. See also A. Elżanowski, Czym jest i czym nie jest dobrostan, (in:) H. Mamzer (ed.), Dobrostan zwierząt. Różne perspektywy, Gdańsk 2018, pp. 51–66.

5 The World Organisation for Animal Health (OIE), Terrestrial Animal Health Code (2018), https://www.oie.int/fileadmin/Home/eng/Health_standards/tahc/2018/en_sommaire.htm (accessed 19.04.2021).

6 *Ibidem*.

7 On this topic, see J. Mason and M. Finelli, Nowa, wspaniała ferma? (in:) P. Singer (ed.), W obronie zwierząt, Warsaw 2011, pp. 152–179; P. Lymbery and I. Oakeshott, Farmagedon. Rzeczywisty koszt taniego mięsa, Białystok 2020, pp. 197–205; D. De Grazia, Prawa zwierząt. Bardzo krótkie wprowadzenie, Krakow 2014, pp. 103–107; E. Herbut and J. Walczak, Dobrostan zwierząt w nowoczesnej produkcji, „Przegląd Hodowlany" 2017, no. 5, pp. 3–7.

fur or eggs. For example, the maximum stocking density for broilers ranges from 33 kg/m^2 to as much as 42 kg/m^2 depending on the requirements met by the poultry house concerned. This means that such a small area can hold up to 17 birds weighing 2.44 kg each (the average weight of a broiler sent to a slaughterhouse in Poland).[8] In such a situation, one chicken has at its disposal an area smaller than A4 size. The situation is no better for laying hens, which may be kept in single- or multi-tier cages or without cages on single or multiple tiers. The cage area per laying hen should be at least 0.075 m^2. In a non-cage system, the maximum stocking density of laying hens per m^2 of floor space in a poultry house is nine hens.[9] Under such conditions, the animals cannot satisfy their ethological needs and are exposed to severe stress, serious physical injury and various infectious diseases.

Another factor affecting the welfare of livestock is genetic selection determining characteristics to meet the demand for meat. For example, fast-growing broilers are used for this purpose in the chicken meat sector in the EU. These birds reach the target weight of 2 to 2.5 kg in about 35–45 days. The genetic selection of broilers over the last few decades has led to a significant increase in their growth rate and meat yield. Today, standard broilers reach a body weight of 1.5 kg in less than 30 days, whereas in the 1950s it took 120 days. The modification of many different metabolic and behavioural traits also leads to various welfare problems in broilers. These include bone deformities, lameness, ascites, sudden death syndrome and contact dermatitis.[10] When discussing the issue of animal welfare in industrial breeding, reference should also be made to animal transport and slaughter, which are essential elements of this production process. During transport, as during rearing, animals are exposed to congestion, hunger, dehydration, inadequate temperatures and various injuries. Moreover, contrary to the current rules, it is common practice in EU countries to transport animals that are unfit for transport to slaughterhouses.[11] Unfortunately, in many cases, animals also bear suffering during slaughter that could be avoided. This is mainly due to the abandonment of the stunning of animals during ritual slaughter or the incorrect stunning of the animal during routine slaughter. According to estimates

8 Krajowa Izba Producentów Drobiu i Pasz, Różnice w wadze i długości chowu brojlerów w Europie, https://archiwum.kipdip.org.pl/article/id/1293 (accessed 19.04.2021).

9 Ordinance of the Minister of Agriculture and Rural Development of 15 February 2010 on the requirements and procedures for keeping farm animal species for which protection standards have been defined in EU law (Journal of Laws 2010, No. 56, item 344, as amended).

10 Report from the Commission to the European Parliament and the Council on the impact of genetic selection on the welfare of chickens kept for meat production, COM/2016/0182 final, Brussels 2016.

11 European Commission, Overview report on systems to prevent the transport of unfit animals in the European Union (DG SANTE, 2015–8721 – MR), Luxembourg 2015, p. Iff., https://op.europa.eu/en/publication-detail/-/publication/2bdfe42c-e33f-409e-8f02–4f0308205ede/language-en (accessed 19.04.2021). See also M. Rudy, Traktat o uśmiercaniu zwierząt, Warsaw 2019, pp. 323–328.

by Stowarzyszenie Otwarte Klatki, in Poland alone, as many as 27 million hens can have full awareness at the time of their slaughter.[12] For the sake of clarity, it should be noted that similar problems apply to all animal species kept in industrial farms.

2. Legal Issues

The improvement of the living conditions of livestock[13] is largely dependent on the applicable legislation currently in force.[14] In the Polish legal order, the basic legislation to regulate these matters is the Act of 21 August 1997 on the protection of animals (hereinafter: APA).[15]This act introduced the principle of the dereification of animals (Article 1(1) APA) and the requirement of humane treatment of animals (Article 5 APA).[16] Of course, this obligation also applies to livestock, which, like other categories of animals, must be treated with their needs taken into account, adequately cared for and protected (Article 4(2) APA). At the same time, the legislature has banned the maltreatment of animals, including the use of cruel methods in the rearing or breeding of animals (Article 6(2) Item 12). These include, in particular, human acts or omissions which clearly lead to pathological changes in the animal's body (whether somatic or psychological), in particular in the form of the effects of suffering severe pain or coercion with hunger, thirst, electrical stimulation (except the use of electric fences, tamers and electrical devices for driving the livestock) or other such procedures, especially the force-feeding and watering of animals (Article 4(7) APA).

The APA also sets out the basic duties of livestock keepers and the minimum conditions for keeping livestock. It is primarily about the obligation to provide farm animals with care and appropriate living conditions, i.e. the possibility of existence

12 Stowarzyszenie Otwarte Klatki, Raport o stanie hodowli brojlerów w Polsce, 2018, pp. 15–17. See also European Commission, Overview report, *op. cit.*; J. Szymborski, Ubój rutynowy a rytualny. Podobieństwa i różnice, "Życie Weterynaryjne" 2015, no. 7, pp. 469–471.

13 This refers to livestock in the meaning of the Act of 10 December 2020 on the organization of breeding and reproduction of livestock (Journal of Laws 2021, item 36).

14 See, for example, M.E. Szymańska, Livestock Welfare: Legal Aspects, (in:) E. Kruk, G. Lubeńczuk and H. Spasowska-Czarny (eds.), Legal Protection of Animals, Lublin 2020, pp. 177–187; S. Mroczkowski, A. Frieske, B. Sitkowska, E. Grochowska and D. Piwczyński, Prawne aspekty humanitarnej ochrony zwierząt, „Przegląd Hodowlany" 2015, no. 2, pp. 34–36; S. Mroczkowski and A. Frieske, Regulacje użytkowania zwierząt, Bydgoszcz 2016, pp. 45–47; S. Mroczkowski and A. Frieske, Prawna ochrona zwierząt gospodarskich, Bydgoszcz 2015, pp. 61–63; I. Lipińska, Z prawnej problematyki dobrostanu zwierząt gospodarskich, „Przegląd Prawa Rolnego" 2015, no. 1, pp. 63–77; E. Jachnik, Zasada dobrostanu zwierząt we Wspólnej Polityce Rolnej Unii Europejskiej, „Studia Iuridica Lublinensia" 2017, no. 1, pp. 287–296.

15 For the consolidated text, see Journal of Laws 2020, item 638.

16 For more on these issues, see J. Białocerkiewicz, Status prawny zwierząt. Prawa zwierząt czy prawna ochrona zwierząt, Toruń 2005, p. 61ff.; M. Goettel, Sytuacja zwierzęcia w prawie cywilnym, Warsaw 2013, p. 37ff; P. Waldau, Prawa zwierząt. Co każdy powinien wiedzieć, Warsaw 2021, p. 99ff.

in accordance with the needs of a given species, breed, sex and age. The conditions for rearing or breeding animals may not cause injuries and bodily damage or other suffering. For example, it is forbidden to stock animals in excess of the space norms defined for a given species, age and physiological condition (Article 12 APA). Detailed requirements in this regard are set out in the ordinance of the Minister of Agriculture and Rural Development of 15 February 2010 on the requirements and procedures for keeping farm animal species for which protection standards have been defined in EU law[17] and the ordinance of the Minister of Agriculture and Rural Development of 28 June 2010 on the minimum conditions for keeping livestock species other than those for which protection standards have been defined in EU law.[18] The first of these ordinances sets out the requirements and procedures for keeping calves, pigs, laying hens and broilers. The second ordinance specifies the minimum conditions for keeping cattle (except calves), horses, sheep, goats, ostriches, quails, guinea fowl, polar foxes, red foxes, raccoon dogs, mink, polecats, rabbits, chinchillas, coypu, deer and fallow deer, turkeys, geese and ducks (in farms keeping at least 100 of these birds) – separately for each species, including the density of animals depending on the housing system. The above-mentioned legal acts contain mainly technical standards and define the technical requirements for premises intended for keeping animals (lighting, air circulation, watering and feeding equipment, heating and cooling systems); minimum space standards depending on the housing system; requirements for protection against unfavourable weather conditions and predatory animals; rules for animal care; rules for dealing with sick and injured animals; cleanliness standards; nutritional requirements; rules for keeping records containing a description of the production system, etc. Generally, these regulations outline the minimum livestock living conditions, which, when complied with, can be referred to as ensuring animal welfare, at least in principle. However, there is doubt as to whether this goal is achievable at all in the environment of an industrial farm, especially if we assume that welfare must be understood as meeting the specific species-related needs of animals in the field of their physiology, aetiology and health. In any case, the livestock-keeping standards defined by the legislature are often criticized by representatives of academia and social organizations whose statutory goal is to protect animals. Additionally, the problem is that farms very often do not comply with these requirements. When looking for the reasons for this, it is first necessary to point to the lack of effective supervision of compliance with the provisions of the APA.[19]

17 Journal of Laws 2010, No. 56, item 344, as amended.

18 For theconsolidated text, see Journal of Laws 2019, item 1966.

19 See Informacja NIK o wynikach kontroli 'Funkcjonowanie nadzoru nad obrotem i ubojem zwierząt rzeźnych ze szczególnym uwzględnieniem dobrostanu zwierząt' (KSR-411400/2004, Ref. no. 201/2004/D04503/KSR), Warszawa, 20 January 2005 r.; Informacja NIK o wynikach kontroli 'Nadzór nad funkcjonowaniem ferm zwierząt', (KRR-4101–01-00/2014, Ref. no. 181/2014/P/14/050/KRR), Warszawa, 12 November 2014; Informacja NIK o wynikach kontroli

Referring to the above, it should be pointed out that under Article 34a(1) APA, compliance with the animal protection rules is supervised by the Veterinary Inspectorate (Inspekcja Weterynaryjna).[20] Pursuant to Article 3 of the Act of 29 January 2004 on the Veterinary Inspectorate, the Veterinary Inspectorate has the responsibility of protecting animal health and the safety of products of animal origin in order to ensure the protection of public health. The essential objective of the Veterinary Inspectorate is therefore to protect human health by protecting animal health; it is not motivated by ethical reasons of protecting animals. It is therefore important to agree with the view that 'there is no public authority in Poland for the supervision of the humane protection of animals, and the Veterinary Inspectorate performs these tasks (if any) only as a spin-off'. This is further supported by the fact that the Veterinary Inspectorate has not been equipped with appropriate powers to play the role assigned to it effectively.[21] For example, it does not have the right to take a maltreated animal away from its owner. This may be all the more surprising given that under Article 7(3) APA, in urgent cases where the continued stay of the animal with the original owner or guardian endangers the animal's life or health, it is police officers, municipal guards and representatives of social organizations whose statutory goal is the protection of animals who are obliged to carry out such activities. Of course, this does not change the fact that under the applicable law, only the Veterinary Inspectorate is authorized to carry out inspection of compliance with the animal protection provisions.

Actual protection of animals also largely depends on legislative measures which allow holding liable those who violate orders or who fail to comply with prohibitions regarding required conduct in the area concerned. The detailed presentation of this complex issue goes far beyond this study. However, it seems necessary to discuss the problem of the penalties for behaviour involving maltreatment of livestock. This need is supported not only by the scientific value of this issue or its social gravity, but also by the interesting results of a study carried out by Fundacja Czarna Owca Pana Kota in partnership with the Stowarzyszenie Ochrony Zwierząt Ekostraż from Wrocław. The research was based on monitoring the activities of courts, prosecutors and the police in animal protection cases, and the findings were published in a report entitled 'Jak Polacy znęcają się nad zwierzętami?' ('How do Poles abuse animals?'). The

'Nadzór nad transportem i ubojem zwierząt gospodarskich' (KRR.430.009.2016, Ref. no. 96/2017/P/16/043/KRR), Warszawa, 7 July 2017.

20 As part of this supervision, the personnel of the Veterinary Inspectorate and persons appointed by the bodies of the Inspectorate have the powers set out in the Act of 29 January 2004 on the Veterinary Inspectorate (consolidated text in the Journal of Laws 2021, item 306).

21 For more on doubts regarding the nature of the (supervisory and auditing) powers held by the Veterinary Inspectorate and the efficiency of its activities, see: W. Radecki, Ustawy o ochronie zwierząt. Komentarz, Warsaw 2015, pp. 204–211; Ł. Smaga, Ochrona humanitarna zwierząt, Białystok 2010, pp. 283–289.

authors point out (among other things) that the suffering of farm animals as a result of human activities is rarely the subject of judicial proceedings,[22] even though these animals constitute the largest group of animals kept by humans, often in conditions which prevent their basic needs being met. Undoubtedly, one of the reasons for this is the construction of the subjective elements of the crime of maltreatment of animals and the resulting criterion of direct action by the offender.

To address this issue, it is necessary to remember that, according to the legal definition, animal maltreatment is understood as consciously inflicting or knowingly allowing pain or suffering, in particular intentionally injuring or mutilating an animal; beating animals; transporting animals in a way causing unnecessary suffering and stress; keeping animals in inappropriate living conditions; abandonment of an animal by the owner or by another guardian; using cruel methods in animal rearing or breeding; exposing an animal to weather conditions that endanger its health or life; or keeping an animal without adequate food or water for a period exceeding the minimum needs appropriate to the species (Article 6(2) Items 1–19 APA). These types of behaviour, as well as the act of unjustified or inhumane killing of animals,[23] are classified as crimes.[24] These are generally defined perpetrator offences prosecuted under public indictment, which may be committed only with intentional fault and also as an aggravated type, i.e. committed with particular cruelty, hence with the use of actions characterized by drastic forms and methods of killing or inflicting suffering, premeditatedly aimed at increasing the extent and duration of suffering.[25] Pursuant to the current wording of Article 35 APA, those acts are punishable by imprisonment for up to three years, and if the perpetrator acts with particular cruelty, they are punishable by imprisonment for a term between three months and five years. In the case of a conviction for this type of offence, the court shall or may

22 For example, a total of 897 cases under the APA were brought to court in the period 2012–2014. Most of these cases concerned pets (83.5%), and a smaller number related to farm animals (12.3%) and wild animals (4.2%). See: D. Karaś, Jak Polacy znęcają się nad zwierzętami? Raport z monitoringu sądów, prokuratur i policji (wersja rozszerzona), Krakow/Wrocław 2016, p. 36ff.; D. Karaś, „Niech zwierzęta mają prawa!" Monitoring ścigania oraz karania sprawców przestępstw przeciwko zwierzętom, „Przegląd Prawa i Administracji" 2017, vol. 108, pp. 17–30.

23 It is worth noting that under the legislation currently in force, the killing of a farm animal for a purpose other than obtaining meat and hides does not benefit from the exclusion of punishability under Article 6(1) Item 1 of the APA and is illegal. For more information, see: M. Rudy, Traktat, *op. cit.*, p. 192ff.

24 For more detail on the statutory elements of offences defined in the APA, see: M. Mozgawa, Prawnokarne aspekty ochrony zwierząt, (in:) M. Mozgawa (ed.), Prawna ochrona zwierząt, Lublin 2002, pp. 168–175; M. Mozgawa, M. Budyn-Kulik, K. Dudka and M. Kulik, Prawnokarna ochrona zwierząt – analiza dogmatyczna i praktyka ścigania przestępstw z art. 35 ustawy z 21.08.1997 r. o ochronie zwierząt, 'Prawo w Działaniu' 2011, vol. 9, pp. 44–50.

25 For more on the aggravated type of the offence under Article 35 APA (acting with particular cruelty), see: M. Gabriel-Węglowski, Przestępstwa przeciwko humanitarnej ochronie zwierząt, Toruń 2008, pp. 104–109.

impose penal measures provided for in the APA, such as forfeiture of the animal, a prohibition on possessing any animal or a specific category of animals, a prohibition on exercising an occupation or activity related to the use of animals or affecting them, and compensation for purposes related to animal protection. These prohibitions are to be imposed in years, from one to fifteen years, and the compensation may be in the amount from PLN 1,000 to PLN 100,000. Less significant infringements of the obligation of humane treatment of animals, in particular concerning the conditions for keeping pets and farm animals, have been classified in Article 37 APA as infractions. For example, it may be noted that the following constitute an infraction: keeping farm animals without providing them with care and appropriate living conditions; fattening geese and ducks for fatty livers; or keeping animals in excess of the room standards defined for a given species, age and physiological state (Article 37 APA).As a rule, these are formal infractions, the essence of which is not dependent on the result.[26] Obviously, if the behaviour specified in Article 37(1) APA has elements of maltreatment of an animal or results in its death inflicted without justification or in an inhumane manner, then a perpetrator acting intentionally will be liable not for the infraction under Article 37(1) APA but for the crime under Article 35 APA. The infractions specified in the APA may be committed both intentionally and unintentionally. For committing such offences, the law provides for the penalty of custody or a fine, as well as the possibility of issuing penal measures (e.g. forfeiture of the animal) and compensation of up to PLN 1,000 for purposes related to animal protection.

Getting back to the above-mentioned problem of the statutory elements of the crime of animal maltreatment, it should be noted that the view that such a crime can only be committed intentionally with direct intent,[27]established in the scholarly opinion and judicature, reduces the criminality of such behaviour only to sadistic acts. In any event, it is difficult to attribute the intention of directly causing pain and suffering to the acts listed in Article 6(2) APA. It is therefore appropriate to accept the postulate proposed in the literature that the legislature should also provide for the possibility of committing acts under Article 6(2) APA with a legal intent (*dolus eventualis*) and that the acts committed with the direct intent (*dolus directus*) of causing pain and suffering should constitute an aggravated offence punishable by a more severe penalty.[28] There is no doubt that such a change would contribute to more effective prosecution and punishment of perpetrators of crimes against

26 On the statutory elements of the infractions under Article 37(1) APA, see for example K. Kuszlewicz, Prawa zwierząt. Praktyczny przewodnik, Warsaw 2019, pp. 193–203.

27 See for examplethe Judgment of the Supreme Court of 14 April 2016, V KK 458/15, LexNo. 2294600.

28 J. Helios and W. Jedlecka, Znęcanie się nad zwierzęciem w doktrynie prawa karnego i w orzecznictwie sądowym – kilka uwag tytułem wstępu do rozważań o prawnej ochronie zwierząt, „Przegląd Prawa i Administracji" 2017, vol. 108, p. 15.

animals. Currently, both the prosecuting authorities and courts very often state that a given act does not meet the criteria of a crime due to the lack of an unambiguous intention of the offender to harm the animal.[29] This happens despite the fact that as early as 2009, the Supreme Court interpreted the provisions of the APA regarding the understanding of the subjective side of the crime of animal maltreatment. This court took a clear position, assuming that 'maltreatment involves… each of the manners of direct conduct towards an animal listed in Article 6(2) of the Act, which must include the direct intent of the perpetrator, the intent therefore referring to the very act of perpetration and not to its effect in the form of suffering or pain'.[30] The Supreme Court's reason for its position was the fact that the pain or suffering of an animal is of an objective nature, and its actual existence is independent of whether the perpetrator directly strived to achieve this goal or not. The object of statutory protection is the protection of animals from suffering and pain, and their suffering in practice does not depend on the motivation of the perpetrator. The Supreme Court thus points out that the understanding of the perpetrator's intent should be placed in a broader context, taking into account the purpose of the APA. This refers primarily to the requirement of humane treatment of all animals (Article 5 APA), which should be understood as treatment that takes into account the needs of the animal and ensures its care and protection (Article 4(2) APA). In other words, the Supreme Court takes the position that in order for the crime in question to occur, it is not necessary for the perpetrator to directly aim at inflicting suffering on the animal. Although the crime of animal maltreatment requires intentional fault on the side of the perpetrator acting with direct intent, this intent should be examined with respect to the very act of perpetration (e.g. failure to feed the animal or keeping it in too dense stock) and not to the perpetrator's intention to inflict pain or suffering. The recognition that 'involuntary' harm is also a crime, when the suffering of the animal is not the goal but a side effect of the perpetrator's actions, is of key importance for the legal protection of livestock. After all, it is rare for keepers of such animals to intentionally inflict pain on them. The suffering of these animals is usually the result of a kind of 'austerity' by the keepers who try to increase the cost-effectiveness of production by, for example, increasing the stocking density of caged animals, reducing expenditure on veterinary care or failing to provide rest periods during transport.

29 See for example theJudgment of the Regional Court in Poznań of 14 June 2018, IV Ka 479/18, LexNo. 2528837.

30 Judgment of the Supreme Court of 16 November 2009, V KK 187/09, Lex No. 553896. See also the Judgment of the Supreme Court of 13 December 2016, II KK 281/16, Lex No. 2237277 and the Judgment of the Supreme Court of 7 July 2020, II KK 222/19, OSNKW 2020, no. 9–10, item 40.

3. Ethical Issues

There is no doubt that moral concern about animals has led to the formulation of various rules ensuring and maintaining their welfare. It is therefore worth noting the ethical aspect of the problems associated with the intensification of livestock production and the implementation of modern animal welfare technologies. This is all the more important because with the development of industrial farming, high-yield animals began to be treated as machines, while the fact they are living beings in need of proper care has been ignored. However, the intended use of these animals does not relieve anyone of the obligation to treat them humanely, and the moral relativism seen in such cases is difficult to justify. The causes of this problem can be found for example in the relaxation of the relationship between human and animal, which in a sense determines the empathy necessary in these relations. Unfortunately, most people currently do not have contact with live animals on a daily basis, but only with more or less processed products of animal origin.

The human attitude towards animals is constantly evolving. It changes with the cultural and civilizational development of societies. In the European cultural circle, the principles of moral behaviour are, to a large extent, determined by Christian ethics. It is therefore worth beginning by pointing out the influence of Christianity on shaping people's attitudes towards animals. This is all the more necessary because of the incorrect opinion, expressed by some, that the Christian religion perpetuates the stereotype of thinking about animals as things and is responsible for the current environmental crisis. Such a view was formulated, among others, by the American historian Lynn White, who, in his article 'The Historical Roots of Our Ecologic Crisis', published in 1967, accused Christianity of orthodox arrogance towards nature and extreme anthropocentrism, as well as of unintentionally contributing to the degradation of the natural environment and its resources. This problem, according to White, is rooted in the Book of Genesis, which, in his view, grants man unlimited power over the world and introduces the Christian axiom that the only reason for the existence of nature is to serve man.[31] It would be difficult, however, to share this view, which is undoubtedly the result of a misunderstanding of the biblical call to 'fill the earth and subdue it' (Gen. 1:28).[32] Moreover, it should be pointed out that the attitude of human domination over nature finds its ideological inspiration outside Christianity, more precisely in the naturalistic concept of individualism and liberalism which dominated European thinking in the 18th century, giving form to a materialistic vision of the world. In any case, one has to agree with Jacek Łapiński,

31 L.T. White, Jr, The Historical Roots of our Ecological Crisis, "Science" 1967, vol. 155, pp. 1205–1207.

32 The Book of Genesis, *New Jerusalem Bible*, https://www.catholic.org/bible/book.php (accessed 19.04.2021).

who argues that it was the influence of materialistically oriented individualism and liberal economics under which 'a socially fixed model of thinking emerged that favoured an attitude of exploitation and domination of humanity over nature'.[33] As for the position of the Catholic Church on the issue in question, it is now perhaps best expressed in the words of Pope Francis, who in his encyclical Laudato si' (entirely devoted to ecology) wrote: 'nowadays we must forcefully reject the notion that our being created in God's image and given dominion over the earth justifies absolute domination over other creatures.… the Bible has no place for a tyrannical anthropocentrism unconcerned for other creatures'.[34]

Two basic trends can be distinguished in the contemporary ethical discussion on animal protection. The first is the trend of respecting animal interests (animal welfare), which developed mainly under the influence of Peter Singer's views. The second is the trend of the protection of animal rights, the main advocate for which is Tom Regan.[35] As regards the first of the aforementioned concepts, its main assumptions are presented by Singer in the book entitled *Animal Liberation*, issued in the United States in 1975. Thanks to this book, millions of people around the world learnt about the shocking scale of animal exploitation in laboratories and on industrial farms. The author, describing human cruelty, points to a kind of 'ethical blindness' and calls for action. Singer argues that a disregard of the suffering of any living creature can by no means be morally justified, and the principle of equality requires that the suffering of any animal, regardless of its nature, is treated like the similar suffering of any other living being.[36]In his opinion, the limit for respecting animal interests is defined only by the ability to experience suffering or pleasure, and all other criteria (such as intelligence or rationality) should be rejected because their use would lead to arbitrary decisions. Singer admits that the inclusion of animals within a principle of equality does not entail the need to equate their rights with those of people or to declare that the life of the animal has the same value as human life. At the same time he warns against species chauvinism (speciesism) based on a conviction about the 'holiness and inviolability' of human life only.[37] According to Singer, most people present such an attitude. In this situation, this author claims, we must incorporate animals into

33 J. Łapiński, Etyczne podstawy prawnej ochrony zwierząt, „Studia z Prawa Wyznaniowego" 2002, vol. 4, p. 153 and the literature cited therein.

34 Encyclical letter Laudato si' of the Holy Father Francis on care for our common home, http://www.vatican.va/content/francesco/en/encyclicals/documents/papa-francesco_20150524_enciclica-laudato-si.html (accessed 19.04.2021), paragraphs 67 and 68; R.F. Sadowski, Filozoficzny spór o rolę chrześcijaństwa w kwestii ekologicznej, Warsaw 2015, pp. 104–111; M. Łuszczyńska, Czyńcie sobie Ziemię poddaną – ekologiczne dylematy w nauczaniu społecznym Kościoła katolickiego, Lublin 2021, *passim*.

35 A. Breczko, Od rzeczy do podmiotu. Praktyczne implikacje etyki ochrony zwierząt, „Białostockie Studia Prawnicze" 2013, vol. 14, p. 19ff.

36 P. Singer, Wyzwolenie zwierząt, Warsaw 2018, p. 61ff.

37 *Ibidem*, p. 72ff.

the circle of our moral community and reject the view that we are allowed to sacrifice their lives to the most trivial purposes.[38] Singer points to medical experiments on animals and industrial animal breeding as the most important manifestations of speciesism. Both of these forms of animal exploitation lead to the suffering of a larger number of animals than other human practices. According to Singer, to eliminate them, we must change the policy of our governments and our customs to the same extent as our diet. If we could eliminate the officially supported and most commonly accepted forms of speciesism, the liquidation of other forms would only be a matter of time.[39]

Much more radical in his views is Tom Regan, who is one of the best-known advocates of animal rights. In his view, the moral value of an animal is objective and in any case is not conditioned by its usefulness to humans. Consequently, in their dealings with animals, humans should be guided by the same moral principles as in human relations. In Regan's opinion, animals have the same rights as humans as regards fundamental questions such as the protection of life. Recognition of these rights should result in a total, uncompromising ban on the use of animals. This applies equally to all possible ways of exploiting them (scientific experiments, food production, sport, etc.).Animals are not a resource that humans can use in any way they wish.[40] Regan clearly condemns such objectification of animals and refers to all manifestations of it as 'absolute injustice', 'barbarism', 'despotic discrimination', 'evil'. This author also argues that reforming the injustice is only extending it.[41] This is why, for example, he does not demand humane treatment of farm animals but a 'complete end to all commerce in the flesh of dead animals'. Moreover, Regan refers to facts to strengthen his arguments, pointing out that about 5 billion animals are bred and killed every year in the USA alone. In his view, this situation will change when the animal rights philosophy prevails. For this to happen, people need to change their beliefs and then their habits, in particular their eating habits.

38 *Ibidem*, p. 75.

39 *Ibidem*, p. 79. See also: T. Turowski, Zmierzch antropocentryzmu w perspektywie etyki nowej Petera Singera, Krakow 2019, p. 13ff.; U. Zarosa, Status moralny zwierząt, Warsaw 2016, pp. 76–86; D. Malinowski, Problematyka podmiotowości prawnej zwierząt na przykładzie koncepcji utylitaryzmu Petera Singera, „Przegląd Prawa Ochrony Środowiska" 2014, no. 2, pp. 185–221.

40 T. Regan, The Case for Animal Rights, (in:) M.W. Fox and L.D. Mickley (eds.), Advances in Animal Welfare Science 1986/87, Dordrecht 1987, p. 179.

41 T. Regan, Filozofia praw zwierząt, (in:) W. Owczarz (ed.), Antologia praw zwierząt, Bielsko-Biała 1995, p. 82. See also: D. Probucka, Prawa zwierząt, Krakow 2015, pp. 107–174; D. Gzyra, Teoria praw zwierząt Toma Regana, (in:) T. Gardocka and A. Gruszczyńska (eds.), Status zwierzęcia. Zagadnienia filozoficzne i prawne, Toruń 2012, pp. 45–60.

4. Public Reception

The presentation of the title issue also requires a reference to the question of the perception of problems related to the industrial breeding of animals. However, the presentation of the findings made in this respect should be preceded by general comments on the level of public awareness of the need for animal protection.[42]This is all the more important because people still show different, often extreme, attitudes towards animals – from reification to personification. Fortunately, however, the awareness of Poles in this area is quite high. This is confirmed by the results of surveys conducted by Centrum Badania Opinii Społecznej (CBOS). In the communication of a survey carried out in August 2018, this foundation pointed out that the vast majority of the respondents (79%) believed that all animals feel pain in the same way as humans. About one in eight (12%) believed that some animals feel pain just as much as humans do, and some feel less. Few (2%) said all animals suffer less pain than humans do.[43]However, it turns out that awareness of the suffering of animals does not translate simply into respondents' views on the admissibility of the use of animals for different purposes or into consumer attitudes. For example,46% of those surveyed believed that keeping animals in zoos is mostly appropriate; 33% of those surveyed believed that testing human medicines on animals is mostly appropriate; 15% believed that animal testing of cosmetics and cleaning products is mostly appropriate. As regards the attitude of respondents towards animal breeding,48% believed that animals should be reared in both industrial and organic farms, so that people have the choice of from what type of farming and at what price they want to buy food; 42% believed that all animals should be reared in an organic way, as animal breeding conditions are more important than the price of food products;5% believed that industrial animal breeding should be widespread so as to make food products as cheap as possible. In this context, the findings on the motives for purchasing decisions are particularly interesting. It turns out that only 7% of Poles were concerned with the issue of animal testing when purchasing cosmetics and cleaning products. The situation is definitely better when it comes to buying eggs; in this case, 35% of the respondents declared that, when purchasing eggs, they pay attention to the conditions under which the hens are reared. It is also worth noting that the importance for consumers of whether eggs come from cage rearing or other systems (organic, free-range, barn rearing) increased almost threefold (i.e. from 13%

42 See for example H. Mamzer, Polacy wobec cierpienia zwierząt, „Życie Weterynaryjne" 2017, no. 11, pp. 796–798.

43 Since 1996, the opinions of those surveyed about the pain suffered by animals have not significantly changed. As before, currently about 80% of the respondents think that animals feel pain in the same way as humans. Other indications remain at the same level. Cf. Postawy wobec zwierząt. Komunikat z badań CBOS (BS/79/2013), Warsaw 2013, p. 1ff.; Postawy wobec zwierząt. Komunikat z badań CBOS (No. 112/2018), Warsaw 2018, p. 1ff.

to 35%)in the period 2006–2018.[44] The CBOS survey respondents were also asked about the environmental impact of industrial rearing. As regards this issue,34% of respondents did not have a firm opinion on the subject; 31% believed that industrial livestock rearing can have a negative impact on the environment (including through high greenhouse gas emissions); 25% believed that industrial livestock rearing has little impact on the environment; and 10% believed that this type of livestock rearing has no impact on the environment whatsoever.[45]

Focusing on the problem of industrial rearing, it is also worth citing the results of a survey carried out in the first half of 2019 by Centrum Badawczo-Rozwojowe BioStat on a representative sample of adult Poles. The survey showed that 48.5% of respondents were against industrial farms, while 37% were in favour of this model of animal production. At the same time, 72.1% of those surveyed believed that chickens reared on industrial farms suffer from the high concentration of animals; 73.1% of respondents believed that breeding and killing animals for their fur should not be allowed in Poland.[46] As it turns out, Poles are largely aware of the health and environmental risks associated with the operation of industrial farms, but do not realize the scale of the phenomenon. Despite associating industrial breeding with high animal density, when answering the question about the maximum allowable stocking density a large proportion of respondents indicated very low values compared to reality. For example, as many as 25.6% of respondents believed that up to 350 chickens should be kept on farms, while currently even up to 1 million chickens are kept on some farms.[47]

Final Remarks

To prevent changes turning agriculture into an industry that is more and more cruel for animals, we need a profound modification of law. Unfortunately, the regulations currently in force which set out the livestock welfare standards are in fact an expression of political clientelism rather than concern for animals. This

44 *Ibidem*, pp. 2–11.

45 *Ibidem*, p. 11.

46 A nationwide trend of public support for the ban on fur farming is also apparent in those municipalities in which many fur farms are located. The factors influencing the opinion of the local communities in this regard include characteristics of the settlement grid, the nuisance of farms to the social and natural environments, the importance of farming to the local economy and the labour market, and the awareness of respondents that farm animals are suffering. See: Mieszkańcy wobec ferm zwierząt futerkowych, Raport z badań w gminach Czerniejewo, Koźmin Wielkopolski i Nowogard, Zachodni Ośrodek Badań Społecznych i Ekonomicznych, *passim*. Cf. M. Michalak and P. Cholewińska, Znaczenie hodowli zwierząt futerkowych w Polsce, „Wiadomości Zootechniczne" 2018, no. 3, pp. 199–202.

47 Sprzeciw społeczny wobec ferm przemysłowych, Raport Koalicji Społecznej Stop Fermom Przemysłowym, 2021, p. 35ff.

is manifested, inter alia, in the protection of the economic interests of certain industries and professional groups, as well as in a willingness to recognize the right of religious minorities to behave contrary to universal norms resulting from human moral development. There is no doubt that the first step to be taken on this path is a radical tightening of the requirements for the living conditions for all species of livestock, a complete ban on breeding animals for fur and a complete ban on killing animals without first rendering them unconscious. The fact that this is possible is best demonstrated by the examples of other countries, such as Great Britain, which banned fur farming in 2000, or Sweden, where ritual slaughter was banned in 1937. The legislature should act with the same resoluteness in this matter as in the case of the technique of forced waterfowl fattening for a fatty liver, which has been prohibited in Poland since 1 January 1999.[48] It is necessary because we are currently facing the greatest ecological crisis in the history of human kind. There is no more time for half-measures, and a profound change is needed in the decades-long models of production and consumption. We must realize that true progress is of a moral nature. This means that it must be done with full respect for the human person and the world of nature. A warning and a guideline in this regard may be the words of Pope Paul VI, who in 1970 spoke about the dire effects of 'industrial civilization', emphasizing the urgent need for a radical change in human behaviour because 'the most extraordinary scientific progress, the most astounding technical feats and the most amazing economic growth, unless accompanied by authentic moral and social progress, will in the long run go against man'.[49]

There is no doubt that the inherent conflict of interests between animal production and the demands of environmental ethics can only be solved in one manner, i.e. by appropriate regulation of human obligations towards animals and liability for non-compliance with these obligations. The development of ethical (philosophical) reflection in this area is of paramount importance, but it is the role of positive law to give a real dimension to the idea of the humane protection of animals by ensuring its implementation.[50] This entails many difficulties. Above all, the development of civilization (including technological progress) is bringing about new moral dilemmas which need to be resolved. However, we do not have a single ethical foundation on which we can base such decisions. On the contrary, with increasing social and cultural diversity, the situation of lawmakers and entities which apply law

48 See: J. Książkiewicz, Historia tuczu przymusowego drobiu wodnego na stłuszczone wątroby – aspekty badawcze i technologiczne, „Wiadomości Zootechniczne" 2006, no. 3, pp. 82–87.

49 Visit of Pope Paul VI to the FAO on the 25th anniversary of its institution, Monday, 16 November 1970, paragraph 4, http://www.vatican.va/content/paul-vi/en/speeches/1970/documents/hf_p-vi_spe_19701116_xxv-istituzione-fao.html (accessed 19.04.2021).

50 A. Marek-Bieniasz, Zaranie, rozwój oraz perspektywy etyki środowiskowej – wybrane zagadnienia, „Studia Ecologiae et Bioethicae" 2014, no. 1, pp. 59–69; T. Przesławski, Rola etyki w systemie prawnym, „Profilaktyka Społeczna i Resocjalizacja" 2015, no. 28, pp. 37–48.

becomes more and more complicated, and these entities should, after all, take into account the varying interests and values of different social groups. Of course, it seems unlikely that legal solutions could be found that would correspond to the moral views of all members of society.[51] Regardless of this, there is no other way than to seek and invoke universal values such as life or freedom from suffering.

As a conclusion, it should also be noted that any attempt to assess the degree of the development of public morality in the field of animal protection cannot be disconnected from basic legal decisions, especially those of an ideological nature. This is so because, as rightly pointed out by T. Pietrzykowski, such regulations 'may be regarded as the expression of a certain public moral consensus'.[52] The best examples of this are Article 1 and Article 5 APA, which implement the principle of the dereification of animals and the requirement for their humane treatment. One should also agree with the view that the axiological foundations of the legal system are usually the 'clearest expression of public acceptance of certain values or principles'.[53] This does not mean that only law expresses it. Besides, in certain situations, e.g. due to the evolution of standards of public morality, positive law may contradict the moral order, which may lead to various social conflicts. Finally, it is also worth keeping in mind that the mere adoption of a law does not guarantee that the law will be observed. For this to happen, it is necessary, inter alia, to develop a moral culture in society, manifested in moral awareness and the ability to implement the applicable moral norms and values.[54]

REFERENCES

Arney D. and Piirsalu P., The Ethics of Keeping Fur Animals: The Estonian Context, "Proceedings of the Latvian Academy of Sciences" 2017, no. 1–2.

Białocerkiewicz J., Status prawny zwierząt. Prawa zwierząt czy prawna ochrona zwierząt, Toruń 2005.

Breczko A., Od rzeczy do podmiotu. Praktyczne implikacje etyki ochrony zwierząt, „Białostockie Studia Prawnicze" 2013, vol. 14.

51 Cf. for example A. Elżanowski, Polskie problemy ochrony zwierząt, http://boz.org.pl/art/polskie_problemy.htm (accessed 29.06.2021); S. Mroczkowski, Ochrona zwierząt w świetle prawa i etyki, "Przegląd Hodowlany" 2017, no. 1, pp. 4–6; D. Arney and P. Piirsalu, The Ethics of Keeping Fur Animals: The Estonian Context, "Proceedings of the Latvian Academy of Sciences" 2017, no. 1–2, pp. 78–80.

52 T. Pietrzykowski, Moralność publiczna a konstytucyjne podstawy ochrony zwierząt, 'Studia Prawnicze' 2019, no. 1, p. 18.

53 *Ibidem*, p. 17.

54 B. Wrona, Pomiędzy racjonalizmem a sentymentalizmem. Rozważania dotyczące norm etycznych odnośnie zwierząt, 'Zeszyty Naukowe Towarzystwa Doktorantów Uniwersytetu Jagiellońskiego' 2011, no. 1, p. 85 and the literature referred to therein.

Broom D.M., A History of Animal Welfare Science, "Acta Biotheoretica" 2011, no. 59.

De Grazia D., Prawa zwierząt. Bardzo krótkie wprowadzenie, Krakow 2014.

Elżanowski A., Czym jest i czym nie jest dobrostan, (in:) H. Mamzer (ed.), Dobrostan zwierząt. Różne perspektywy, Gdańsk 2018.

Elżanowski A., Polskie problemy ochrony zwierząt, http://boz.org.pl/art/polskie_problemy.htm.

Encyclical letter Laudato si' of the Holy Father Francis on care for our common home, http://www.vatican.va/content/francesco/en/encyclicals/documents/papafrancesco_20150524_enciclica-laudato-si.html.

Gabriel-Węglowski M., Przestępstwa przeciwko humanitarnej ochronie zwierząt, Toruń 2008.

Goettel M., Sytuacja zwierzęcia w prawie cywilnym, Warsaw 2013.

Grabowska B., Zmiany relacji człowiek – zwierzę, czyli cena postępu, „Kultura i Wartości" 2014, no. 2.

Gzyra D., Teoria praw zwierząt Toma Regana, (in:) T. Gardocka and A. Gruszczyńska (eds.), Status zwierzęcia. Zagadnienia filozoficzne i prawne, Toruń 2012.

Harari Y.N., Industrial farming is one of the worst crimes in history, "The Guardian" 25 September 2015, https://www.theguardian.com/books/2015/sep/25/industrial-farming-one-worst-crimes-history-ethical-question.

Helios J. and Jedlecka W., Znęcanie się nad zwierzęciem w doktrynie prawa karnego i w orzecznictwie sądowym – kilka uwag tytułem wstępu do rozważań o prawnej ochronie zwierząt, „Przegląd Prawa i Administracji" 2017, vol. 108.

Herbut E., Walczak J., Dobrostan zwierząt w nowoczesnej produkcji, „Przegląd Hodowlany" 2017, no. 5.

Jachnik E., Zasada dobrostanu zwierząt we Wspólnej Polityce Rolnej Unii Europejskiej, „Studia Iuridica Lublinensia" 2017, no. 1.

Karaś D., 'Niech zwierzęta mają prawa!' Monitoring ścigania oraz karania sprawców przestępstw przeciwko zwierzętom, „Przegląd Prawa i Administracji" 2017, vol. 108.

Karaś D., Jak Polacy znęcają się nad zwierzętami? Raport z monitoringu sądów, prokuratur i policji (wersja rozszerzona), Krakow/Wrocław 2016.

Książkiewicz J., Historia tuczu przymusowego drobiu wodnego na stłuszczone wątroby – aspekty badawcze i technologiczne, „Wiadomości Zootechniczne" 2006, no. 3.

Kuszlewicz K., Prawa zwierząt. Praktyczny przewodnik, Warsaw 2019.

Lipińska I., Z prawnej problematyki dobrostanu zwierząt gospodarskich, „Przegląd Prawa Rolnego" 2015, no. 1.

Lymbery P. and Oakeshott I., Farmagedon. Rzeczywisty koszt taniego mięsa, Białystok 2020.

Łapiński J., Etyczne podstawy prawnej ochrony zwierząt, „Studia z Prawa Wyznaniowego" 2002, vol. 4.

Łuszczyńska M., Czyńcie sobie Ziemię poddaną – ekologiczne dylematy w nauczaniu społecznym Kościoła katolickiego, Lublin 2021.

Malinowski D., Problematyka podmiotowości prawnej zwierząt na przykładzie koncepcji utylitaryzmu Petera Singera, „Przegląd Prawa Ochrony Środowiska" 2014, no. 2.

Mamzer H., Polacy wobec cierpienia zwierząt, 'Życie Weterynaryjne' 2017, no. 11.

Marek-Bieniasz A., Zaranie, rozwój oraz perspektywy etyki środowiskowej – wybrane zagadnienia, „Studia Ecologiae et Bioethicae" 2014, no. 1.

Mason J. and Finelli M., Nowa, wspaniała ferma? (in:) P. Singer (ed.), W obronie zwierząt, Warsaw 2011.

Michalak M. and Cholewińska P., Znaczenie hodowli zwierząt futerkowych w Polsce, „Wiadomości Zootechniczne" 2018, no. 3.

Mozgawa M., Budyn-Kulik M., Dudka K. and Kulik M., Prawnokarna ochrona zwierząt – analiza dogmatyczna i praktyka ścigania przestępstw z art. 35 ustawy z 21.08.1997 r. o ochronie zwierząt, „Prawo w Działaniu" 2011, vol. 9.

Mozgawa M., Prawnokarne aspekty ochrony zwierząt, (in:) M. Mozgawa (ed.), Prawna ochrona zwierząt, Lublin 2002.

Mroczkowski S. and Frieske A., Prawna ochrona zwierząt gospodarskich, Bydgoszcz 2015.

Mroczkowski S. and Frieske A., Regulacje użytkowania zwierząt, Bydgoszcz 2016.

Mroczkowski S., Ochrona zwierząt w świetle prawa i etyki, „Przegląd Hodowlany" 2017, no. 1.

Mroczkwoski S., Frieske A., Sitkowska B., Grochowska E., Piwczyński D., Prawne aspekty humanitarnej ochrony zwierząt, „Przegląd Hodowlany" 2015, no. 2.

Pietrzykowski T., Moralność publiczna a konstytucyjne podstawy ochrony zwierząt, „Studia Prawnicze" 2019, no. 1.

Probucka D., Prawa zwierząt, Krakow 2015.

Przesławski T., Rola etyki w systemie prawnym, „Profilaktyka Społeczna i Resocjalizacja" 2015, no. 28.

Radecki W., Ustawy o ochronie zwierząt. Komentarz, Warsaw 2015.

Regan T., Filozofia praw zwierząt, (in:) W. Owczarz (ed.), Antologia praw zwierząt, Bielsko-Biała 1995.

Regan T., The Case for Animal Rights, (in:) M.W. Fox and L.D. Mickley (eds.), Advances in Animal Welfare Science 1986/87, Dordrecht 1987.

Rudy M., Traktat o uśmiercaniu zwierząt, Warsaw 2019.

Sadowski R.F., Filozoficzny spór o rolę chrześcijaństwa w kwestii ekologicznej, Warsaw 2015.

Singer P., Wyzwolenie zwierząt, Warsaw 2018.

Smaga Ł., Ochrona humanitarna zwierząt, Białystok 2010.

Szymańska M.E., Livestock Welfare: Legal Aspects, (in:) E. Kruk, G. Lubeńczuk and H. Spasowska-Czarny (eds.), Legal Protection of Animals, Lublin 2020.

Szymborski J., Ubój rutynowy a rytualny. Podobieństwa i różnice, „Życie Weterynaryjne" 2015, no. 7.

The Book of Genesis, *New Jerusalem Bible*, https://www.catholic.org/bible/book.php.

Turowski T., Zmierzch antropocentryzmu w perspektywie etyki nowej Petera Singera, Krakow 2019.

Visit of Pope Paul VI to the FAO on the 25th anniversary of its institution, Monday, 16 November 1970, http://www.vatican.va/content/paul-vi/en/speeches/1970/documents/hf_p-vi_spe_19701116_xxv-istituzione-fao.html.

Waldau P., Prawa zwierząt. Co każdy powinien wiedzieć, Warsaw 2021.

White L.T., Jr, The Historical Roots of our Ecological Crisis, "Science" 1967, vol. 155.

Wrona B., Pomiędzy racjonalizmem a sentymentalizmem. Rozważania dotyczące norm etycznych odnośnie zwierząt, „Zeszyty Naukowe Towarzystwa Doktorantów Uniwersytetu Jagiellońskiego" 2011, no 1.

Zarosa U., Status moralny zwierząt, Warsaw 2016.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2021 vol. 26 nr 3

sciendo

DOI: 10.15290/bsp.2021.26.03.11

Received: 20.02.2021
Accepted: 17.05.2021

Cezary Kulesza
Uniwersytet w Białymstoku, Polska
c.kulesza@uwb.edu.pl
ORCID ID: https://orcid.org/0000–0003-0509–327X

Rozprawa zdalna oraz zdalne posiedzenie aresztowe w świetle konwencyjnego standardu praw oskarżonego

Remote Trial and Remote Detention Hearing in Light of the ECHR Standard of the Rights of the Accused

Abstract: This article concerns the compliance of the institutions of remote trials and remote detention hearings introduced to the CCP by the Polish 'coronavirus act' of 19 June 2020 with the ECHR standard on the rights of the accused. In the first part of the article, it is indicated that the ECtHR in its jurisprudence accepts that a trial in the form of a videoconference is not in principle contrary to the ECHR, provided, however, that there are compelling reasons to dispense with the traditional trial (main or appellate) and that the procedure of using a videoconference itself meets the requirements of a fair trial according to Article 6 ECHR and ensures the accused both effective personal participation in the trial and effective use of the services of a defence counsel, in particular the confidentiality of the lawyer's contact with their client. The Covid-19 outbreak has changed European justice systems, and now videoconferencing in court proceedings is seen not only as an exceptional measure, but as possibly an effective part of the ordinary activity of courts. The analysis of the assumptions of remote trials in ordinary Polish criminal proceedings shows that this institution does not meet the standards of a fair trial, especially the standard of the effective participation of the defence counsel. In contrast, compared to a remote trial, a remote detention hearing in Poland has a wider scope of application and poses serious risks to the standards on deprivation of liberty (Article 5(3) and Article 3 ECHR) and effective defence (Article 6(3) ECHR). The possibility of using both forms of videoconferencing without the participation of a defence counsel and the permanent nature of the changes introduced are particularly worrying.
Keywords: ECHR, ECtHR, effective defence, fair trial, videoconference
Słowa kluczowe: EKPC, ETPC, efektywna obrona, rzetelny proces, videokonferencja

Wprowadzenie

Celem artykułu jest zbadanie, czy polskie uregulowania rozprawy zdalnej i zdalnego posiedzenia aresztowego spełniają standardy rzetelnego procesu i ochrony praw oskarżonego przewidziane w Europejskiej Konwencji Praw Człowieka (dalej EKPC) oraz oparte na niej orzecznictwo Europejskiego Trybunału Praw Człowieka. W związku z powyższym należy na początku zbadać, czy orzecznictwo ETPC stworzyło taki standard bazujący na specyficznych cechach rozprawy zdalnej prowadzonej w formie wideokonferencji i czy jest on aktualny w krajach europejskich w dobie epidemii spowodowanej koronawirusem COVID-19. Następnie podstawowe założenia tego standardu należy odnieść do wspomnianych regulacji polskich wprowadzonych „ustawą covidową" z 19 czerwca 2020 r., przede wszystkim w aspekcie prawa oskarżonego do obrony.

Należy zauważyć, że fundamenty rzetelnego procesu we wszystkich sprawach karnych określa przede wszystkim art. 6 EKPC oraz oparte na tym przepisie orzecznictwo Europejskiego Trybunału Praw Człowieka (powoływanym dalej jako ETPC). Art. 6 ust. 1 Konwencji stanowi w zdaniu pierwszym, że: „Każdy ma prawo do rzetelnego *(fair)* i publicznego rozpatrzenia jego sprawy w rozsądnym terminie przez niezawisły i bezstronny sąd ustanowiony ustawą przy rozstrzyganiu o jego prawach i obowiązkach o charakterze cywilnym albo o zasadności każdego oskarżenia w wytoczonej przeciwko niemu sprawie karnej". W zdaniu drugim określa się także zasadę jawności postępowania sądowego, od której ustawodawca krajowy może wprowadzić wyjątki. Z kolei art. 6 ust. 2 EKPC określa zasadę domniemania niewinności, a art. 6 ust. 3 zasadę prawa oskarżonego do obrony, przewidując w literach a–e gwarancje tego prawa. W rezultacie z całokształtu norm przewidzianych w art. 6 EKPC wyprowadza się w orzecznictwie ETPC i literaturze przedmiotu zasadę bądź model rzetelnego procesu (*fair trial*)[1].

W literaturze oprócz praw *stricte* odnoszących się do oskarżonego, w tym gwarancji rzetelnego procesu, wyróżnia się pakiet praw chroniących oskarżonego incydentalnie, w związku ze stosowaniem poszczególnych instytucji karnoprocesowych[2]. W tym ostatnim aspekcie istotne są prawa oskarżonego odnoszące się do pozbawienia wolności oskarżonego w toku postępowania karnego (art. 5 ust. 1–5 EKPC) oraz zakaz tortur, nieludzkiego lub poniżającego traktowania lub karania (art. 3 EKPC). Szczególne znaczenie mają tu standardy dotyczące aresztu określone w art. 5 ust. 3 i 4 EKPC, dotyczące odpowiedniej procedury sądowej zarówno stosowania aresztu, jak

1 Zob. P. Wiliński, Pojęcie rzetelnego procesu karnego, (w:) P. Wiliński (red.), A. Błachnio-Parzych, J. Kosonoga, H. Kuczyńska, C. Nowak, P. Wiliński, Rzetelny proces karny w orzecznictwie sądów polskich i międzynarodowych, Warszawa 2009, s. 19–34.

2 M. Wąsek-Wiaderek, Standard ochrony praw oskarżonego w świetle Europejskiej Konwencji Praw Człowieka, (w:) C. Kulesza (red.), Strony i inni uczestnicy procesu karnego, t. VI, P. Hofmański (red.), System prawa karnego procesowego, Warszawa 2016, s. 530–531.

i odwołania od decyzji o aresztowaniu[3]. W związku z powyższym w artykule podjęto także próbę krótkiej analizy, czy takie standardy pozbawienia wolności spełnia zdalne posiedzenie aresztowe, przede wszystkim standard udziału obrońcy w postępowaniu aresztowym określony przez orzecznictwo ETPC odnoszące się do art. 5 ust. 4 EKPC.

1. Rozprawa zdalna w świetle standardu rzetelnego procesu

Wśród gwarancji prawa do obrony zawartych w art. 6 ust. 3 EKPC za istotne z punktu widzenia udziału oskarżonego w rozprawie w sposób zdalny należy uznać prawo oskarżonego do:

„c) bronienia się osobiście lub przez ustanowionego przez siebie obrońcę, a jeśli nie ma wystarczających środków na pokrycie kosztów obrony – do bezpłatnego korzystania z pomocy obrońcy wyznaczonego z urzędu, gdy wymaga tego dobro wymiaru sprawiedliwości;
d) przesłuchania lub spowodowania przesłuchania świadków oskarżenia oraz żądania obecności i przesłuchania świadków obrony na takich samych warunkach jak świadków oskarżenia".

Europejski Trybunał Praw Człowieka generalnie uznaje w swoim orzecznictwie, że wideokonferencja jako forma udziału oskarżonego w postępowaniu karnym zasadniczo nie jest niezgodna z pojęciem rzetelnej i publicznej rozprawy sądowej. Jednakże zdaniem Trybunału zastosowanie tej technologii w każdym przypadku musi służyć uzasadnionemu celowi, a procedury składania wyjaśnień przez oskarżonego i jego udział w rozprawie muszą być zgodne z wymogami rzetelnego procesu, określonymi w art. 6, i zapewniać oskarżonemu skuteczne prawo do obrony. W szczególności należy umożliwić oskarżonemu śledzenie postępowania i bycie wysłuchanym bez przeszkód technicznych, a także zapewnić mu skuteczną i poufną komunikację z obrońcą[4]. Podwaliny standardu rzetelnej rozprawy zdalnej stworzyło orzecznictwo ETPC w sprawach włoskich, przede wszystkim w sprawach *Viola v. Włochy*[5] i *Asciutto v. Włochy*[6].

3 Zob. M.A. Nowicki, Komentarz do art. 5 EKPC, (w:) M.A. Nowicki, Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka, wyd. VII, WKP 2017 i podane tam orzecznictwo ETPC.

4 ECHR, Guide on Article 6of the European Conventionon Human Rights, Right to a fair trial (criminal limb), Strasbourg, Updated on 30 April 2021, s. 33, 88 i podane tam orzecznictwo ETPC; https://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf (10.06.2021).

5 Wyrok ETPC z 5 października 2006 r. w sprawie *Marcello Viola v. Włochy*, skarga nr 45106, HUDOC (9.06.2021).

6 Wyrok ETPC z 27 listopada 2007 r. w sprawie *Asciutto v. Włochy*, skarga nr 35795/02 HUDOC (9.06. 2021).

Przed przejściem do tych orzeczeń wypada wskazać, że instytucja rozprawy w formie wideokonferencji jest stosowana we włoskim procesie karnym od roku 1998. W szczególności wprowadzony wówczas art. 146 bis przepisów wykonawczych do k.p.k. wskazuje dokładnie przypadki zastosowania wideokonferencji (w sprawach najpoważniejszej przestępczości zorganizowanej o charakterze mafijnym, handlu narkotykami i terrorystycznej), właściwy organ do zarządzania takiej konferencji oraz techniczne warunki połączenia audiowizualnego. Ponadto ustawą nr 103/2017 ustawodawca włoski znacznie rozszerzył zakres stosowania art. 146 bis, wskutek czego stosowanie wideokonferencji nie jest już wyjątkowe, lecz stało się regułą w stosunku do aresztowanych lub skazanych za najcięższe przestępstwa. W przypadku więźniów odbywających karę w zaostrzonym rygorze ich udział w rozprawach i posiedzeniach możliwy jest jedynie w formie wideokonferencji, przy jednoczesnym zapewnieniu im prawa do korzystania z pomocy obrońcy (w tym z urzędu) i poufnego kontaktu z adwokatem[7]. W obu włoskich sprawach: *Marcello Viola* i *Asciutto*, dotyczących zorganizowanej (mafijnej) przestępczości ETPC stwierdził, że udział skarżących w rozprawach za pomocą wideokonferencji służył uzasadnionym, uznanym przez EKPC celom, a mianowicie obronie porządku publicznego, zapobieganiu przestępczości, ochronie prawa do życia, wolności oraz bezpieczeństwu świadków i ofiar przestępstw, a także poszanowaniu wymogu „rozsądnego terminu" w odniesieniu do długości postępowań sądowych. Badając z kolei procedurę wideokonferencji, Trybunał uznał ją za spełniającą wymogi rzetelnego procesu, gdyż oskarżeni korzystali z pomocy obrońców, mieli możliwość składania oświadczeń z miejsca swego pobytu, odbierali bez zakłóceń dźwięk i obraz z rozprawy i sami byli widziani i słyszani przez sąd oraz uczestników procesu. Ponadto w sprawie *Viola* obrońca oskarżonego mógł również wysłać swojego substytuta do sali, na której przebywał oskarżony uczestniczący w wideokonferencji, lub postąpić odwrotnie – osobiście zająć się swoim klientem i powierzyć zastępującemu go adwokatowi obronę swojego klienta przed sądem[8].

W innych sprawach Trybunał zauważał, że trudności w porozumiewaniu się na odległość oskarżonego w sposób zdalny z sądem powinny być kompensowane przez przyznanie oskarżonemu obrońcy[9]. Z kolei w orzecznictwie ETPC dotyczącym spraw apelacyjnych w Rosji Trybunał podkreślał, że relacja między adwokatem a jego klientem powinna opierać się na wzajemnym zaufaniu i zrozumieniu. W związku z powyższym ETPC w sprawie *Sakhnovskiy v. Rosja* wskazał, że warunkiem rzetelności rozprawy zdalnej jest zapewnienie uczestniczącemu w niej oskarżonemu możli-

7 A. Mangiaracina, Report on Italy, (w:) S. Quattrocolo, S. Ruggeri (red.), Personal Participation in Criminal Proceedings. A Comparative Study of Participatory Safeguards and *in absentia* Trials in Europe, Springer 2019, s. 249–251.

8 *Marcello Viola v. Włochy*, § 67–69 i 75–77; *Asciutto v. Włochy*, § 68–72.

9 Wyrok ETPC z 26 czerwca 2008 r. w sprawie *Shulepov v. Rosja*, skarga nr 15435, § 34–39, HUDOC (1.03.2021 r.); zob. także orzecznictwo ETPC w sprawach rosyjskich w: A. Lach, Rzetelne postępowanie dowodowe w świetle orzecznictwa strasburskiego, Warszawa 2018, s. 104.

wości nieskrępowanego i poufnego kontaktu z obrońcą. Zdaniem Trybunału narusza zasadę rzetelnego procesu sytuacja, gdy poufności tego kontaktu nie gwarantuje korzystanie z łączy wideo obsługiwanych przez pracowników rządu bez wykluczenia możliwości jego niejawnego nadzorowania (podsłuchu i podglądu) i niezapewnienia na przykład kontaktu telefonicznego[10]. W późniejszej sprawie *Gorbunov i Gorbaczov v. Rosja*, podobnie jak w sprawie *Sakhnovskiy*, skarżący był w stanie porozumieć się ze swoim nowo wyznaczonym adwokatem jedynie tuż przed rozpoczęciem rozprawy apelacyjnej. Chociaż z oświadczeń stron złożonych w sprawie *Gorbunov i Gorbaczov* nie wynikało jasno, czy czas wyznaczony na taką komunikację był wystarczający, aby skarżący omówił sprawę i upewnił się, że wiedza jego adwokata na temat sprawy oraz sytuacji prawnej skarżącego jest odpowiednia, główną przyczyną uznania przez Trybunał procedury wideokonferencji za nierzetelną było niezapewnienie poufności kontaktu obrońca – oskarżony. W sprawie tej mogli oni bowiem rozmawiać ze sobą tylko za pomocą łącza wideo. Dodatkowo Trybunał zauważył, że przeprowadzenie wideokonferencji nie było uzasadnione ważną przyczyną, gdyż oskarżony i jego obrońca przebywali w mieście Wołogda, gdzie miał siedzibę sąd apelacyjny, a więc nie było żadnych przeszkód, aby obaj uczestniczyli w rozprawie apelacyjnej bezpośrednio[11].

Warto dodać, że niezapewnienie poufności kontaktu oskarżony – obrońca w trakcie wideokonferencji było podstawą skutecznych skarg do ETPC nie tylko w sprawach przeciwko Rosji. W sprawie *Zagaria v. Włochy*, ETPC stwierdził naruszenie gwarantowanej przez powołany wcześniej art. 146 bis przepisów wykonawczych do włoskiego k.p.k. zasady poufności kontaktu telefonicznego obrońcy w trakcie wideokonferencji przez podsłuchanie rozmowy adwokata z oskarżonym przez funkcjonariusza służby więziennej a następnie sporządzenie przez niego notatki z tej rozmowy dla kierownictwa więzienia Ascoli Piceno. W sprawie tej obrońca oskarżonego występował przed ławą przysięgłych, a oskarżony znajdował się więzieniu, łącząc się z salą rozpraw za pomocą łączy audio-wideo. Mimo że ETPC podzielił stanowisko rządu, że podsłuchana rozmowa nie miała bezpośredniego związku z istotą zarzutów lub strategią obrony, to jednak ostatecznie uznał, że ten bezprawny podsłuch naruszył prawo skarżącego do skutecznego wykonywania prawa do obrony i w związku z tym doszło do naruszenia art. 6 ust. 3 lit. c Konwencji w związku z art. 6 ust. 1[12]. Należy także dodać, że ETPC w sprawach rosyjskich uznaje przeprowadzenie rozprawy w formie wideokonferencji z oskarżonym umieszczonym w metalowej

10 Wyrok ETPC z 27 listopada 2018 r., 39159/12, *Sakhnovskiy v. Rosja*, § 98, 102–104, HUDOC (3.03.3021) i podane tam orzecznictwo ETPC.

11 Wyrok ETPC z 1 marca 2016 r. w sprawie *Gorbunov i Gorbaczov v. Rosja*, skargi nr 43183/06 and 27412/07, § 37–39, HUDOC (15.06.2021).

12 Wyrok ETPC z 27 listopada 2007 r. w sprawie *Zagaria v. Włochy*, skarga nr 58295/00, § 32–36, HUDOC (10.06.2021).

klatce za sprzeczne z zakazem tortur lub nieludzkiego bądź poniżającego traktowania (art. 3 EKPC)[13]. Ponadto w wielu swoich orzeczeniach ETPC wskazywał jako argument za dopuszczalnością wideokonferencji fakt, że stanowi ona ważny instrument międzynarodowej pomocy prawnej przewidziany m.in. przez Europejską Konwencję z 29 maja 2000 r. o pomocy prawnej w sprawach karnych pomiędzy Państwami Członkowskimi UE (art. 10)[14], a w literaturze zaleca się jej stosowanie jako efektywnego instrumentu współpracy sądowej na przykład w sprawach dotyczących europejskiego nakazu aresztowania[15].

Podsumowując powyższe rozważania, można stwierdzić, że ETPC akceptował co do zasady prowadzenie rozpraw sądowych w formie wideokonferencji jako wyjątków od tradycyjnej rozprawy, ale przy zaistnieniu ważnych, uznawanych przez EKPC przyczyn *(compelling reasons)* i zapewnieniu oskarżonemu gwarancji rzetelnego procesu właściwym właśnie tradycyjnej rozprawie. W literaturze zachodniej zauważa się, że prawa z art. 6 EKPC nie mają charakteru absolutnego i powinny być zrównoważone z innymi prawami chronionymi przez EKPC. W dobie pandemii COVID-19 prawa wynikające z rzetelnego procesu muszą być zrównoważone przez ustawodawców i sądy z ochroną zdrowia publicznego i z absolutnym prawem do samego życia[16]. Dlatego też należy zauważyć, że w trakcie epidemii COVID-19 w europejskich systemach wymiaru sprawiedliwości wideokonferencja stała się jedyną możliwą formą prowadzenia rozprawy, która zapewniała względną ochronę sądowi i uczestnikom postępowania przed zarażeniem wirusem. To właśnie względy ochrony życia i zdrowia sędziów i innych uczestników procesu stały się *ex definitione* „*compelling reasons*" odejścia od tradycyjnej formy bezpośredniej i publicznej rozprawy na rzecz wideokonferencji, która to technologia umożliwiła odblokowanie europejskich systemów wymiaru sprawiedliwości. Ich działalność została bowiem zawieszona na czas pandemii w krajach europejskich bądź na mocy ustaw, bądź też wskutek braku aktywności parlamentów – w drodze aktów administracyjnych o randze podustawowej[17]. Dodać należy, że nie bez znaczenia jest fakt, że w dobie pandemii sam ETPC również przeprowadza swoje rozprawy w budynku w Strasburgu z użyciem wideokonferencji (zob. np. wyrok ETPC z 1 czerwca 2021 r. w sprawie *Denis and Irvine v. Belgia*, skarga nr 62819/17 i 63921/17, § 9). Ponadto należy wskazać, że zgodnie z art. 15 EKPC

13 Wyrok ETPC z 26 marca 2019 r. w sprawie *Valyuzhenich v. Rosja*, skarga nr 10597/13, § 25–26, HUDOC (10.06.2021).

14 Ratyfikowana przez Polskę 27 lipca 2007 r. (Dz.U. z 2007 r. Nr 135, poz. 590); zob. także P. Gori, A. Pahladsingh, Fundamental rights under Covid-19: an European perspective on videoconferencing in court, ERA Forum 2021, vol. 21, s. 567.

15 Zob. G. Jansen, The need for a new roadmap of procedural safeguards: a lawyer's perspective, ERA Forum 2021, published on-line 12.05.2021, Springer.

16 P. Gori, A. Pahladsingh, Fundamental…, *op. cit.*, s. 567.

17 Odnośnie do Włoch, Danii i innych krajów zob. P. Gori, A. Pahladsingh, Fundamental…, *op. cit.*, s. 561–564.

państwo członkowskie może podjąć środki uchylające je z zobowiązań wynikających z Konwencji w przypadku wojny lub innego zagrożenia publicznego zagrażającego egzystencji narodu. Od początku ogłoszenia przez Światową Organizację Zdrowia pandemii dziewięć państw, które już wiosną 2020 r. ogłosiły na swoim terytorium stan wyjątkowy, a mianowicie Albania, Armenia, Gruzja, Estonia, Łotwa ,Mołdawia, Rumunia, San Marino i Serbia, skorzystało z tego prawa[18]. Jednakże w literaturze poświęconej analizie ustawodawstwa „covidowego" w krajach europejskich generalnie zauważano, że stosowanie wideokonferencji zamiast tradycyjnej rozprawy powinno spełniać standardy rzetelnego procesu wypracowane na tle art. 6 EKPC[19]. Jeśli chodzi o samą procedurę stosowania wideokonferencji podnoszono konieczność używania specjalistycznego sprzętu audio-wideo, zauważając jednocześnie, że nie przy wszystkich czynnościach sądowych stosowanie wideokonferencji jest dobrym rozwiązaniem. W tym ostatnim względzie zaproponowano podział czynności sądowych na trzy grupy: a) czynności sądowe *(hearing activities*), które mogą być wykonywane w drodze wideokonferencji tak samo dobrze albo nawet lepiej niż w sposób konwencjonalny, b) czynności, które można przeprowadzić przy pomocy takiego narzędzia, ale wymaga to uwzględnienia związanych z tym komplikacji oraz c) czynności, które nie są kompatybilne z wideokonferencją i nie powinny być wykonywane przy jej zastosowaniu[20]. Jako przykłady czynności pierwszej grupy wskazuje się sytuacje, w których wideokonferencja mogłaby zapewnić ochronę prawa do obrony jako sposób na zmniejszenie dyskomfortu, spowodowanego na przykład podróżą tymczasowo aresztowanego do wyznaczonego przez sędziego miejsca w celu złożenia oświadczeń lub naradzania się z sędzią delegowanym innym niż osoba uprawniona do decydowania. Jeśli chodzi o czynności drugiej grupy, gdzie wideokonferencja powoduje komplikacje, wskazuje się postępowania z wieloma oskarżonymi i stronami, zwłaszcza jeśli wymagają one tłumaczy. Powstaje wtedy sytuacja wymagająca nawiązywania nie tylko połączeń „punkt-punkt", między dwoma lub kilkoma lokalizacjami, ale także połączeń wielopunktowych, jednocześnie między wieloma lokalizacjami, i w związku z tym bez zapewnienia odpowiedniego skonfigurowania sieci specjalistycznych urządzeń powstaje poważne ryzyko niespełnienia warunków efektywnego udziału w takich czynnościach wszystkich uczestników konferencji. Do grupy trzeciej, a więc czynności, przy których wideokonferencja jest formą nieprzydatną, zalicza się konfrontację sądową świadków (oskarżenia i obrony) lub oskarżonych ze

18 Zob. O. Kaplina, S. Sharenko, Access to Justice in Ukrainian Criminal Proceedings During the Covid-19 Outbreak, Access to Justice in Eastern Europe, 2020, Issue 2/3 (7), s. 119–121; A. Boskovic, T. Kesic, Questioning Defendants via Skype during the State of Emergency in the Republic of Serbia, Journal of Liberty and International Affairs (JLIA) 2020, vol. 6, nr Thematic Issue, s. 30–44.

19 O. Kaplina, S. Sharenko, Access…, *op. cit.*, s. 125–126; P. Gori, A. Pahladsingh, Fundamental…, *op. cit.*, s. 570–574.

20 P. Gori, A. Pahladsingh, Fundamental…, *op. cit.*, s. 576–577.

względu na psychologiczne implikacje oceny sądowej wiarygodności konfrontowanych uczestników procesu, nieograniczającej się do zwykłego sprawdzenia logicznej, wewnętrznej spójności treści każdego oświadczenia. Doświadczenia w stosowaniu wideokonferencji wskazują także na to, że jest ona bardziej efektywna, jeśli przeprowadza się ją na wniosek stron i uczestników procesu, a nie na mocy arbitralnej decyzji sądu[21].

2. Ewolucja rozprawy zdalnej w polskim procesie karnym

Tak zwana „rozprawa odmiejscowiona" została wprowadzona do polskiego k.p.k. ustawą z 31 sierpnia 2011 r.[22], stanowiącą część tzw. Pakietu UEFA EURO 2012, i z założenia miała stanowić instrument zwalczania przede wszystkim przestępczości stadionowej. Pomijając podnoszoną w komentarzach niefortunność użytego w projekcie ustawy terminu „rozprawa odmiejscowiona"[23], należy wskazać, że jej założeniem jest prowadzenie rozprawy w dwóch różnych miejscach (miejscu przebywania oskarżonego i siedzibie sądu) połączonych za pomocą urządzeń umożliwiających przekazywanie obrazu i dźwięku na odległość. W sytuacji zdecydowania przez sąd o takiej rozprawie można odstąpić od przymusowego doprowadzenia do sądu sprawcy ujętego na gorącym uczynku bądź w bezpośrednim pościgu, jeśli zostanie zapewnione uczestniczenie przez sprawcę w sposób zdalny we wszystkich czynnościach sądowych, w których ma on prawo uczestniczyć, w szczególności złożenie przez niego wyjaśnień (art. 517 b, § 2a k.p.k.). W czynnościach wideokonferencji w miejscu przebywania sprawcy bierze udział referendarz sądowy lub asystent sędziego zatrudniony w sądzie, w którego okręgu przebywa sprawca. Natomiast jeśli w sprawie został ustanowiony obrońca, uczestniczy on w czynnościach prowadzonych w sposób zdalny w miejscu przebywania sprawcy. Nie rozwijając opisu „rozprawy odmiejscowionej" w trybie przyspieszonym (oraz zgodności z zasadą domniemania niewinności używania przez ustawodawcę terminu „sprawca"), która stała się pierwowzorem opisywanej dalej rozprawy zdalnej w postępowaniu zwyczajnym, należy wskazać na przesłanki jej wprowadzenia[24]. Przede wszystkim należy zauważyć, że w obecnym kształcie tryb przyspieszony jest fakultatywny, może być stosowany jedynie w sprawach o mniejszym trybie gatunkowym, charakteryzujących się

21 *Ibidem*, s. 577.

22 Ustawa z 31 sierpnia 2011 r. o zmianie ustawy o bezpieczeństwie imprez masowych oraz niektórych innych ustaw, Dz.U. Nr 217, poz. 1280 – ustawa weszła w życie 12 listopada 2011 r.

23 A.R. Światłowski, (w:) J. Skorupka (red.), Kodeks postępowania karnego. Komentarz, wyd. 3, Warszawa 2018, s. 1203.

24 Na temat uzasadnienia wprowadzenia rozprawy „odmiejscowionej" zob. J. Kosowski, Rozprawa „odmiejscowiona", „Prokuratura i Prawo" 2012, nr 1, s. 37–40 oraz D. Morgała, Rozprawa odmiejscowiona jako środek walki z chuligaństwem stadionowym?, „Czasopismo Prawa Karnego i Nauk Penalnych" 2012, z. 3, s. 125–126.

nieskomplikowanym charakterem, skutkującym możliwością ich szybkiego rozpoznania, a zdalne przeprowadzenie rozprawy umożliwia rezygnację z zatrzymywania oskarżonego i doprowadzania do sądu[25]. Jednakże w komentarzach do tej instytucji zgłaszane są uwagi krytyczne dotyczące w przypadku asystenta sędziego i referendarza sądowego braku instrumentów służących zapewnieniu przez nich prawidłowości czynności sądowych przeprowadzanych zdalnie i ograniczenia efektywnego udziału obrońcy w takich czynnościach w miejscu pobytu oskarżonego wynikające z braku jego bezpośredniego kontaktu z sądem, co nie spełnia postulatu „równości broni" obrony i oskarżenia[26].

W kontekście konwencyjnych gwarancji rzetelnego procesu sądowego należy wskazać, że nowelizacja k.p.k. dokonana ustawą „covidową" z 19 czerwca 2020 r.[27] rozszerzyła instytucję rozprawy „odmiejscowionej" stosowanej w trybie przyspieszonym na rozprawy prowadzone w postępowaniu zwyczajnym. W nowych paragrafach 3–9 art. 374 k.p.k. przewidziano możliwość zdalnego uczestniczenia w rozprawie nie tylko oskarżonego i jego obrońcy, lecz także oskarżyciela publicznego, posiłkowego i prywatnego oraz tłumacza. Zgodnie z uzasadnieniem projektu ustawy celem nowelizacji było „(...) poszerzenie możliwości zdalnego przeprowadzania wybranych czynności postępowania karnego, co służyć będzie zwiększeniu jego szybkości, zmniejszeniu kosztów i uciążliwości ponoszonych przez uczestników procesu w związku z koniecznością stawiennictwa w sądzie, a równocześnie stworzy możliwości ograniczenia zagrożeń wynikających ze stanu epidemii dla osób uczestniczących w tych czynnościach w charakterze organu procesowego lub uczestnika" [28]. Tak więc można uznać, że cele wprowadzenia tej instytucji do postępowania zwyczajnego odpowiadają konwencyjnemu standardowi „ważnego powodu" (*compelling reason)* odejścia od tradycyjnej formy rozprawy sądowej. Przy ocenie instytucji rozprawy zdalnej należy jednak zauważyć uprzywilejowanie prokuratora wobec innych stron i uczestników procesu, gdyż jego wniosek o umożliwienie mu udziału w rozprawie w formie wideokonferencji jest dla sądu wiążący, co stanowi nieuzasadniony przejaw dominacji oskarżyciela publicznego nad przewodniczącym i sądem będącym wszak *dominus litis* rozprawy sądowej[29]. Jednakże zgodnie z założeniem arty-

25 Zob. np. B. Skowron, (w:) K. Dudka (red.), Kodeks postępowania karnego. Komentarz, wyd. 2, Warszawa 2020, s. 1127 i podana tam literatura.

26 A.R. Światłowski, *op. cit.*, s. 1204.

27 Ustawa z 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19 (Dz.U. poz. 1086) – ustawa weszła w życie 24 czerwca 2020 r.

28 Druk Sejmowy nr 382, Sejm VIII Kadencji, Warszawa 2020, s. 25.

29 Jak stanowi nowy paragraf 3 art. 374 k.p.k.: „ Przewodniczący, na wniosek prokuratora, **wyraża zgodę** (podkr. CK) na jego udział w rozprawie przy użyciu urządzeń technicznych, umożliwiających udział w rozprawie na odległość z jednoczesnym bezpośrednim przekazem obrazu i dźwięku, jeżeli nie stoją temu na przeszkodzie względy techniczne". Nie wydaje się wystarczają-

kułu ograniczymy się do analizy zdalnego udziału w rozprawie oskarżonego i jego obrońcy w kontekście opisanego wcześniej standardu rzetelnego procesu[30]. Nowy paragraf 4 art. 374 k.p.k. upoważnia przewodniczącego do zapewnienia oskarżonemu pozbawionemu wolności (podobnie jak oskarżycielowi posiłkowemu i prywatnemu) możliwości udziału w rozprawie przy użyciu urządzeń technicznych bezpośrednio przekazujących na odległość obraz i dźwięk jako alternatywy obowiązkowego stawiennictwa na rozprawie. Decyzja przewodniczącego może być podjęta zarówno z urzędu, jak i na wniosek pozbawionego wolności oskarżonego. Zgodnie z art. 374 §1 *in principio* zakres stosowania instytucji zdalnej rozprawy wobec oskarżonego dotyczy jedynie jego obowiązkowego udziału w rozprawie („Przewodniczący może zwolnić z obowiązku stawiennictwa na rozprawie oskarżonego…"), który może wynikać z samej ustawy bądź kiedy przewodniczący lub sąd uznają udział oskarżonego w rozprawie za obowiązkowy (art. 374 §1 i 1a k.p.k.). W komentarzach wskazuje się także, że obowiązek doprowadzenia oskarżonego na rozprawę, w której jego udział nie jest obowiązkowy, powstaje także wtedy, gdy oskarżony złożył wniosek o doprowadzenie w trybie art. 353 § 3 k.p.k. Przyjmuje się więc, że w tych trzech przypadkach zamiast doprowadzenia na salę rozpraw przewodniczący może zarządzić udział oskarżonego w rozprawie przy użyciu urządzeń technicznych w miejscu przebywania oskarżonego [31]. Trudno zgodzić się z tym poglądem w świetle regulacji art. 374 §1 k.p.k., z którego można wywieść, że osobisty i bezpośredni udział oskarżonego w rozprawie jest jego prawem, a więc jeśli oskarżony jest pozbawiony wolności, może żądać doprowadzenia go na rozprawę i wówczas nie można poprzestać na zapewnieniu mu udziału w formie wideokonferencji[32]. Podobnie jak w przypadku „rozprawy odmiejscowionej" w trybie przyspieszonym nad prawidłowością przeprowadzania w sposób zdalny rozprawy czuwać mają referendarz sądu lub asystent sędziego biorący w niej udział w miejscu przebywania oskarżonego, lecz pozbawieni stosownych instrumentów mogących służyć realizacji ich zadań.

Jeśli chodzi o gwarantowane oskarżonemu w art. 6 ust. 3 lit. c EKPC prawo do korzystania z pomocy obrońcy, to udział obrońcy nie jest obligatoryjny i to jemu po-

cym ograniczeniem tej kompetencji prokuratora (nieograniczonej żadnymi przesłankami skorzystania z niej) zgłaszany w doktrynie postulat, aby w tym przepisie termin „wniosek prokuratora" zastąpić terminem „uzasadniony wniosek prokuratora"; zob. Ł. Brzezowski, Udział prokuratora w rozprawie i posiedzeniu zdalnym, „Prokuratura i Prawo" 2021, nr 3, s. 37–40. Warto dodać, że ta nieuzasadniona kompetencja prokuratora jako jeden z przejawów dominacji prokuratury w procesie karnym była przejawem żywej krytyki ze strony uczestników konferencji „Czy proces karny stał się procesem prokuratora ?", zorganizowanej on-line 11 czerwca 2021 r. przez Katedrę Postępowania Karnego WPiA UMCS w Lublinie.

30 Na temat udziału wszystkich uczestników procesu w rozprawie zdalnej zob. np. C. Kulesza, (w:) K. Dudka (red.), Kodeks postępowania karnego. Komentarz, wyd. 3, s. 826–829.

31 D. Świecki, Komentarz do art. 374, (w:) D. Świecki (red.) Kodeks postępowania karnego, t. I. Komentarz aktualizowany, LEX/El 2020.

32 C. Kulesza, (w:) K. Dudka (red.), Kodeks…, *op. cit*., s. 828.

zostawiono wybór miejsca przebywania w trakcie rozprawy prowadzonej w sposób zdalny (w sądzie czy w miejscu pobytu oskarżonego). Wydaje się jednak, że swoją decyzję obrońca powinien uzgodnić z oskarżonym i mieć z nim w trakcie rozprawy kontakt bezpośredni bądź telefoniczny. Warto jednak zauważyć, że oba warianty pobytu obrońcy oskarżonego w trakcie rozprawy prowadzonej w sposób zdalny przewidziane w § 6 art. 374 k.p.k. mają swoje wady: jeśli obrońca znajduje się w miejscu pobytu oskarżonego, rodzi to wskazane wcześniej wątpliwości (na tle trybu przyspieszonego) w kontekście zachowania wymogów efektywnej obrony i zasady kontradyktoryjności. Ponadto należy wskazać na trudności, jakie może napotkać obrońca, związane z podróżą do często odległych od sądu aresztów śledczych czy zakładów karnych. Natomiast w przypadku, gdy obrońca przebywa w trakcie takiej rozprawy w siedzibie sądu, utrudnione może być utrzymywanie bieżącego i poufnego kontaktu telefonicznego z oskarżonym, szczególnie istotnego na przykład w trakcie przesłuchiwania świadków, biegłych czy współoskarżonych. W takich sytuacjach nawet przewidziana w § 7 art. 374 k.p.k. możliwość zarządzenia przerwy przez sąd w celu umożliwienia kontaktu telefonicznego może okazać się niewystarczająca. Ponadto regulacja ta daje sądowi możliwość nieuwzględnienia wniosku obrony o przerwę, jeśli jego złożenie w sposób oczywisty nie służy realizacji prawa do obrony, a w szczególności zmierza do zakłócenia lub nieuzasadnionego przedłużenia rozprawy. Biorąc pod uwagę podkreślaną w orzecznictwie ETPC poufność stosunku obrończego i taktyki obrony, nie wiadomo, na jakich konkretnych przesłankach sąd miałby podejmować decyzję o odmowie zarządzenia przerwy w oparciu o tak generalnie zakreślone kryterium. Jest to istotny problem, gdyż biorąc pod uwagę literalne brzmienie tego przepisu, należy uznać, że o zarządzeniu przerwy decyduje sąd (a nie przewodniczący), a więc negatywna decyzja sądu w przedmiocie wniosku obrony będzie niezaskarżalna. W związku z powyższym naruszenie prawa do obrony w drodze takiej decyzji może być podniesione jedynie w apelacji na podstawie art. 447 § 4 k.p.k.[33]

Udział obrońcy w rozprawie zdalnej jest bardzo istotny także ze względu na treść § 7 art. 374 k.p.k. nakazującego odpowiednie stosowanie art. 517ea k.p.k., z czego wynika ustna forma rozprawy zdalnej. Podczas takiej rozprawy uczestnicy postępowania mogą składać wnioski i inne oświadczenia oraz dokonywać czynności procesowych wyłącznie ustnie do protokołu. Odpowiednie stosowanie tej regulacji oznacza także, że o treści wszystkich pism procesowych, które wpłynęły do akt sprawy od chwili przekazania do sądu aktu oskarżenia, sąd jest obowiązany poinformować oskarżonego oraz jego obrońcę i na żądanie obrony sąd ma obowiązek odczytać treść tych pism (art. 517 § 1ea). Ponadto zgodnie z art. 517 § 2ea na rozprawie mogą być odczytywane te pisma procesowe oskarżonego i jego obrońcy, których nie można było przekazać do sądu. W komentarzach wskazuje się, że chodzi tu o przeszkody w prze-

33 J. Zagrodnik, Komentarz do art. 374, (w:) J. Skorupka (red.), Kodeks postępowania karnego. Komentarz aktualizowany, wyd. 33, Legalis.

kazywaniu pism natury faktycznej, wynikające z odległości między oboma miejscami przeprowadzania rozprawy zdalnej[34].

Zdaniem Helsińskiej Fundacji Praw Człowieka pozostawienie w art. 374 § 7 k.p.k. w rękach sądu możliwości decydowania o tym, kiedy kontakt obrońcy z klientem jest zasadny, stanowił będzie prostą drogę do naruszenia prawa do obrony i regulację tę trudno pogodzić nie tylko z wymogami, które stawia art. 6 § 3 lit. c Konwencji, ale także wymogami dyrektywy Parlamentu Europejskiego i Rady 2013/48/UE z 22 października 2013 r. w sprawie prawa dostępu do adwokata w postępowaniu karnym i w postępowaniu dotyczącym europejskiego nakazu aresztowania[35].

3. Udział oskarżonego w zdalnym posiedzeniu aresztowym w świetle konwencyjnego standardu pozbawiania wolności

Orzecznictwo ETPC przeniosło zasadę równouprawnienia stron jako element rzetelnego procesu także na postępowania incydentalne, czyniąc z niej element standardu pozbawienia wolności[36]. W komentarzach do EKPC zauważa się, że co do zasady art. 5 ust. 4 nie wymaga obligatoryjnego ustanawiania obrońcy w ramach sądowego postępowania kontrolnego, niemniej w niektórych sytuacjach ustanowienie przedstawiciela procesowego może okazać się konieczne dla zapewnienia realności ochrony prawnej, w szczególności wówczas, gdy osoba pozbawiona wolności z uwagi na swój wiek względnie stan psychiczny nie jest w stanie samodzielnie zaprezentować swoich argumentów. Jednakże jeśli w sprawie występuje obrońca, postępowanie może być uznane za odpowiadające standardowi jedynie wtedy, gdy obrońca może swobodnie komunikować się z osobą aresztowaną w celu przygotowania strategii obrony.[37] W orzecznictwie ETPC podkreśla się, że efektywność kontroli sądowej zagwarantowanej w art. 5 ust. 4 Konwencji wymaga ochrony poufności wymiany informacji między oskarżonym pozbawionym wolności i broniącym go adwokatem.

34 A.R. Światłowski, *op. cit*., s. 1211.

35 Uwagi Helsińskiej Fundacji Praw Człowieka z 14 czerwca 2020 r., Druk Senacki nr 142, s. 7–8; https://www.hfhr.pl/wp-content/uploads/2020/06/druk-senacki-nr-142-uwagi-HFPC-1.pdf (25.01.2021).

36 J. Matras, Standard „równości broni" w postępowaniu w przedmiocie tymczasowego aresztowania, „Prokuratura i Prawo" 2009, nr 3, s. 5–11 i podane tam orzecznictwo ETPC i literatura.

37 P. Hofmański, Komentarz do art. 5 EKPC, (w:) L. Garlicki (red.), Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, tom I. Komentarz do artykułów 1–18, Legalis 2010 i podane tam orzecznictwo ETPC; zob. także B. Gronowska, Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z 31.01.2002 r. w sprawie *Lanz p. Austrii* (dot. kontroli zasadności stosowania aresztu tymczasowego oraz prawa osoby tymczasowo aresztowanej do swobodnych kontaktów z obrońcą), „Prokuratura i Prawo" 2002, z. 5, s. 133.

Pomoc obrońcy jest nieefektywna, jeśli nie może on rozmawiać ze swoim klientem i otrzymać od niego poufnych instrukcji bez żadnej kontroli[38].

Wprowadzone ustawą z 19 czerwca 2020 r. zdalne posiedzenie aresztowe zostało ukształtowane podobnie jak rozprawa prowadzona w sposób zdalny, z tym że oczywiście dotyczy ono jedynie podejrzanego (oskarżonego). Nowy paragraf b art. 250 k.p.k. przewiduje możliwość odstąpienia od przymusowego doprowadzenia do sądu podejrzanego, jeżeli zostanie zapewniony jego udział w posiedzeniu, w szczególności złożenie przez niego wyjaśnień, przy użyciu urządzeń technicznych umożliwiających przeprowadzenie tego posiedzenia na odległość z jednoczesnym bezpośrednim przekazem obrazu i dźwięku. W takim posiedzeniu bierze udział w miejscu przebywania podejrzanego referendarz sądowy lub asystent sędziego, a jeżeli podejrzany przebywa w zakładzie karnym lub areszcie śledczym – funkcjonariusz Służby Więziennej. Biorąc pod uwagę, że szczególnie w sytuacji, kiedy sąd orzeka w przedmiocie przedłużenia aresztu, zasadą będzie pobyt podejrzanego (oskarżonego) w areszcie lub zakładzie karnym, i wówczas regułą będzie właśnie udział w posiedzeniu zdalnym funkcjonariuszy Służby Więziennej, którzy nie dają takich gwarancji bezstronności i swobody wyjaśnień podejrzanego jak referendarz sądowy czy asystent sędziego. Podobnie jak w przypadku rozprawy prowadzonej w sposób zdalny obrońca bierze udział w posiedzeniu w miejscu przebywania oskarżonego bądź w sądzie. Jednakże swoboda wyboru przez obrońcę miejsca przebywania może być ograniczona przez sąd, który ma uprawnienie do zobowiązania go do udziału w posiedzeniu w budynku sądu z uwagi na niebezpieczeństwo nierozstrzygnięcia wniosku w przedmiocie zastosowania tymczasowego aresztowania przed upływem dopuszczalnego czasu zatrzymania oskarżonego (art. 250 § 2d k.p.k.). W wypadku, gdy obrońca przebywa w innym miejscu niż oskarżony, kodeks przewiduje możliwość zarządzenia przez sąd na wniosek obrony przerwy i zezwolenia na kontakt telefoniczny oskarżonego z obrońcą. Nie powtarzając wcześniejszych uwag co do uznaniowości sądu przy decydowaniu o umożliwieniu takiego kontaktu i jego poufności, należy dodać, że w tym przypadku kryterium nieuwzględnienia wniosku stanowi nie tylko możliwość zakłócenia prawidłowego przebiegu posiedzenia, lecz także „ryzyko nierozstrzygnięcia wniosku w przedmiocie zastosowania tymczasowego aresztowania przed upływem dopuszczalnego czasu zatrzymania podejrzanego" (art. 250 § 3e k.p.k.).

Należy wskazać, że nowe regulacje ograniczają i tak skromne gwarancje udziału obrońcy w posiedzeniu aresztowym, szczególnie przy pierwszym stosowaniu najostrzejszego środka zapobiegawczego (zob. niezmieniony art. 249 § 3 k.p.k.) Ponieważ warunkiem efektywnego udziału obrońcy w posiedzeniu aresztowym jest

38 Wyrok ETPC z dnia 10 maja 2007 r. w sprawie *Modârcă v Mołdawii* skarga nr 14437/05, § 87–89, HUDOC (30.07.2021) oraz wyrok ETPC z 31 stycznia 2002 r. w sprawie *Lanz v Austrii*, skarga nr 24430/94, § 41–45, HUDOC (30.07.2021).

znajomość akt postępowania przygotowawczego, należy dostrzec praktyczne trudności w zapoznawaniu się z tym aktami wynikające z ograniczeniami ich dostępności w sądzie w okresie 24 godzin, jaki ma sąd na rozpoznanie wniosku o areszt[39]. W rezultacie w przypadku zdalnego posiedzenia aresztowego obrońca, mając do wyboru albo zaznajomienie się z aktami sprawy, albo podróż do aresztu lub zakładu karnego celem udziału w posiedzeniu w miejscu przebywania oskarżonego, najczęściej wybierze pobyt w siedzibie sądu (lub zostanie do tego zobowiązany przez sąd). W tym ostatnim przypadku nie będzie on najczęściej w stanie nawiązać bezpośredniego kontaktu z oskarżonym przed posiedzeniem, zaś kontakt telefoniczny w trakcie posiedzenia, zależny od uznaniowej decyzji sądu, może być niewystarczający. W rezultacie naruszony zostaje standard efektywnego dostępu podejrzanego pozbawionego wolności do obrońcy[40]. Dlatego też w komentarzach zauważa się, że przepisy o zdalnym posiedzeniu aresztowym w nieproporcjonalny sposób ograniczają prawo oskarżonego do obrony (bez względu na to, czy jest on zarażony wirusem COVID-19, czy nie), pozbawiając go możliwości kontaktu z ustanowionym obrońcą i udziału urzędnika sądowego w miejscu, gdzie przebywa podejrzany[41]. Na koniec należy dodać, że w orzecznictwie ETPC w sprawach rosyjskich podkreśla się, że przebywanie oskarżonego w trakcie zdalnego posiedzenia aresztowego w metalowej klatce wprawdzie nie narusza standardu z art. 5 ust. 3 i 4 , ale narusza zakaz z art. 3 ETPC[42].

Wnioski końcowe

ETPC w czasach przed pandemią COVID-19 tradycyjnie wymagał, aby przeprowadzenie rozprawy zdalnej znajdowało uzasadnienia w postaci „ważnego powodu" *(compelling reason)*. Ponadto, zdaniem Trybunału, ograniczenia osobistej obrony oskarżonego wynikające z oddalenia jego miejsca pobytu od sądu powinny być kompensowane przez umożliwienie mu kontaktu z obrońcą, przy zapewnieniu jego poufności. Z kolei oceniając instytucję zdalnego posiedzenia aresztowego, należy zauważyć, że w porównaniu ze zdalną rozprawą ma ona szerszy zakres stosowania, gdyż w przypadku orzekania przez sąd w przedmiocie aresztu regułą jest wcześniejsze pozbawienie wolności oskarżonego (w trybie zatrzymania bądź aresztu). Niedopuszczalne jest odbywanie takiego posiedzenia w formie wideokonferencji jedynie w przypadku oskarżonego wskazanego w art. 79 § 1 pkt 2, czyli takiego, który jest głu-

39 Zob. np. C. Kulesza, Rola obrońcy w czynnościach sądowych w postępowaniu przygotowawczym, (w:) Wybrane aspekty nowelizacji prawa karnego, Biuro RPO, Warszawa 2015, s. 93–96.

40 Zob. M. Wąsek-Wiaderek, Standard…, *op. cit.*, s. 589–591 i podane tam orzecznictwo ETPC; zob. także wyrok ETPC z 28 listopada 2017 r. w sprawie *N. v. Rumunia*, skarga nr 59152/08, § 197.

41 J. Skorupka, Komentarz do art. 250, (w:) J. Skorupka (red.), Kodeks…, *op. cit*.

42 Wyrok z 17 kwietnia 2018 r. w sprawie *Karachentsev v. Rosja*, skarga nr 23229/11, § 51–54, HUDOC (10.06.2021).

chy, niemy lub niewidomy (art. 250 § 3f k.p.k.). Wydaje się, że w tym przypadku istnieją poważne niebezpieczeństwa dla standardów pozbawienia wolności (art. 5 ust. 3 i 3 EKPC) i efektywnego korzystania z pomocy obrońcy (art. 6 ust. 3 EKPC), szczególnie w sytuacji pierwszego stosowania aresztu (art. 249 § 3 k.p.k.). Warto dodać, że polski proces karny w zakresie kontaktu osoby aresztowanej z obrońcą nie spełnia nie tylko standardu ECHR[43], ale i standardu unijnego (nieanalizowanego w artykule) korzystania z pomocy obrońcy przez osobę pozbawioną wolności, wynikającego z dyrektywy UE 2013/48/UE z 22 października 2013 r. i dyrektywy (UE) 2016/1919 z 26 października 2016 r. (w zakresie pomocy prawnej z urzędu)[44]. W przypadku zdalnego posiedzenia aresztowego należy podkreślić brak bezpośredniego kontaktu oskarżonego z obrońcą i trudności obrony związane z zaznajomieniem z aktami sprawy. Zarówno w przypadku rozprawy zdalnej, jak i zdalnego posiedzenia aresztowego decyzja sądu o nieuwzględnieniu wniosku obrony o zarządzenie przerwy celem telefonicznego kontaktu obrońcy z oskarżonym przebywających w różnych miejscach jest niezaskarżalna w drodze zażalenia. Poza tym trudno doszukać się przekonującego uzasadnienia wprowadzonych ustawą „covidową" regulacji, biorąc pod uwagę, że nie mają one charakteru incydentalnego (na czas pandemii), lecz trwały, ich stosowanie nie jest uzależnione ani od stanu zdrowia oskarżonego, ani od tego, czy korzysta on z pomocy obrońcy. Przy krytycznej ocenie komentowanych regulacji rozprawy zdalnej nie sposób nie uwzględnić nie tylko braku ustawowych przesłanek odejścia od tradycyjnej formy rozprawy w polskim k.p.k., ale i przytaczanych wcześniej trudności technicznych związanych z przeprowadzaniem niektórych czynności rozprawy, których nieuwzględnienie może powodować, że wideokonferencja nie spełni konwencyjnych wymogów rzetelnej rozprawy. Wideokonferencja nie jest „lekiem na całe zło" rzeczywistości „covidowej" i „pocovidowej" nie tylko w przypadku rozprawy, ale i posiedzenia aresztowego. Jedynie tytułem przykładu można podać, że nawet „covidowe" ustawodawstwo Ukrainy (która nie wprowadziła stanu wyjątkowego i nie skorzystała z art. 15 EKPC) nie przewiduje możliwości przeprowadzenia pierwszego posiedzenia sądu w przedmiocie aresztu w formie wideokonferencji (uznając, że ten instrument nie spełnia wymogów art. 5 EKPC), zaś posiedzenia w przedmiocie przedłużania aresztu mogą się odbywać w drodze wideokonferencji jedynie za zgodą oskarżonego[45].

43 Zob. np. decyzję ETPC z 28 sierpnia 2012 r. w sprawie *Simons v. Belgia*, skarga nr 71407/10, HUDOC (20.06.2021).

44 Zob. np. C. Kulesza, Reformy procesu karnego z perspektywy obrońcy, (w:) C. Kulesza, A. Sakowicz (red.), Ewolucja polskiego wymiaru sprawiedliwości w latach 2013–2018 w świetle standardów rzetelnego procesu, Białystok 2019, s. 95–104.

45 O. Kaplina, S. Sharenko, Access…, *op. cit.*, s. 125–126.

BIBLIOGRAFIA

Boskovic A., Kesic T., Questioning Defendants via Skype during the State of Emergency in the Republic of Serbia, Journal of Liberty and International Affairs (JLIA) 2020, vol. 6, nr Thematic Issue.

Brzezowski Ł., Udział prokuratora w rozprawie i posiedzeniu zdalnym, „Prokuratura i Prawo" 2021, nr 3.

Druk Sejmowy nr 382, Sejm VIII Kadencji, Warszawa 2020.

ECHR, Guide on Article 6of the European Conventionon Human Rights, Right to a fair trial (criminal limb), Strasbourg,Updated on 30 April 2021, https://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf.

Garlicki L. (red.), Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1–18, Legalis 2010.

Gori P., Pahladsingh A., Fundamental rights under Covid-19: an European perspective on videoconferencing in court, ERA Forum 2021, vol. 21.

Gronowska B., Wyrok Europejskiego Trybunału Praw Człowieka w Strasburgu z 31.01.2002 r. w sprawie *Lanz p. Austrii* (dot. kontroli zasadności stosowania aresztu tymczasowego oraz prawa osoby tymczasowo aresztowanej do swobodnych kontaktów z obrońcą), „Prokuratura i Prawo" 2002, z. 5.

Hofmański P., Komentarz do art. 5 EKPC, (w:) L. Garlicki (red.), Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, t. I. Komentarz do artykułów 1–18, Legalis 2010.

Jansen G., The need for a new roadmap of procedural safeguards: a lawyer's perspective, ERA Forum 2021, published on-line 12.05.2021, Springer.

Kaplina O., Sharenko S., Access to Justice in Ukrainian Criminal Proceedings During the Covid-19 Outbreak, Access to Justice in Eastern Europe, 2020, Issue 2/3 (7).

Kosowski J., Rozprawa „odmiejscowiona", „Prokuratura i Prawo" 2012, nr 1.

Kulesza C., (w:) K. Dudka (red.) Kodeks postępowania karnego. Komentarz, wyd. 3, Warszawa 2020.

Kulesza C., Reformy procesu karnego z perspektywy obrońcy, (w:) C. Kulesza, A. Sakowicz (red.), Ewolucja polskiego wymiaru sprawiedliwości w latach 2013–2018 w świetle standardów rzetelnego procesu, Białystok 2019.

Kulesza C., Rola obrońcy w czynnościach sądowych w postępowaniu przygotowawczym, (w:) Wybrane aspekty nowelizacji prawa karnego, Biuro RPO, Warszawa 2015.

Lach A., Rzetelne postępowanie dowodowe w świetle orzecznictwa strasburskiego, Warszawa 2018.

Mangiaracina A., Report on Italy, (w:) S. Quattrocolo, S. Ruggeri (red.), Personal Participation in Criminal Proceedings. A Comparative Study of Participatory Safeguards and *in absentia* Trials in Europe, Springer 2019.

Matras J., Standard „równości broni" w postępowaniu w przedmiocie tymczasowego aresztowania, „Prokuratura i Prawo" 2009, z. 3.

Morgała D., Rozprawa odmiejscowiona jako środek walki z chuligaństwem stadionowym?, „Czasopismo Prawa Karnego i Nauk Penalnych" 2012, z. 3.

Nowicki M.A., Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka, wyd. VII, WKP 2017.

Skorupka J., Komentarz do art. 250, (w:) J. Skorupka (red.), Kodeks postępowania karnego. Komentarz aktualizowany, wyd. 33, Legalis.

Skowron B., (w:) K. Dudka (red.), Kodeks postępowania karnego. Komentarz, wyd. 2, Warszawa 2020.

Światłowski A.R., (w:) J. Skorupka (red.), Kodeks postępowania karnego. Komentarz, wyd. 3, Warszawa 2018.

Świecki D., Komentarz do art. 374, (w:) D. Świecki (red.), Kodeks postępowania karnego, t. I. Komentarz aktualizowany, LEX/El 2020.

Uwagi Helsińskiej Fundacji Praw Człowieka z 14 czerwca 2020 r., Druk Senacki nr 142, https://www.hfhr.pl/wp-content/uploads/2020/06/druk-senacki-nr-142-uwagi-HFPC-1.pdf.

Wąsek-Wiaderek M., Standard ochrony praw oskarżonego w świetle Europejskiej Konwencji Praw Człowieka, (w:) C. Kulesza (red.), Strony i inni uczestnicy procesu karnego, t. VI, P. Hofmański (red.) System prawa karnego procesowego, Warszawa 2016.

Wiliński P., Pojęcie rzetelnego procesu karnego, (w:) P. Wiliński (red.), A. Błachnio-Parzych, J. Kosonoga, H. Kuczyńska, C. Nowak, P. Wiliński, Rzetelny proces karny w orzecznictwie sądów polskich i międzynarodowych, Warszawa 2009.

Zagrodnik J., Komentarz do art. 374, (w:) J. Skorupka (red.), Kodeks postępowania karnego. Komentarz aktualizowany, wyd. 33, Legalis.

Contributors

Anetta Breczko is Associate Professor and Head of the Institute of Theory and Philosophy of Law in the Department of Historical and Legal Sciences, Theory and Philosophy of Law, and Comparative Law at the Faculty of Law, University of Białystok, Poland.

Patrycja Dąbrowska-Kłosińska is Assistant Professor in the Faculty of Administration and Social Sciences at the Warsaw University of Technology and Research Fellow at the School of Law, Queen's University Belfast.

Wojciech Filipkowski is Associate Professor and Head of the Laboratory of Forensic Science in the Faculty of Law, University of Białystok, Poland.

Agnieszka Grzelak is Associate Professor at the College of Law, Kozminski University, Warsaw.

Wioleta Hryniewicka-Filipkowska is Assistant Professor in the Department of Public International Law at the Faculty of Law, University of Białystok, Poland.

Emil Kruk is Assistant Professor in the Department of Administrative Law and Administration and Public Law at the Faculty of Law and Administration, Maria Curie-Sklodowska University, Poland.

Cezary Kulesza is Professor and Head of the Department of Criminal Procedure in the Faculty of Law, University of Białystok, Poland.

Arianna Maceratini is Researcher in Philosophy of Law and Adjunct Professor of Legal Informatics in the Department of Law, University of Macerata, Italy.

Agnieszka Nimark is a Visiting Scholar at the Reppy Institute for Peace and Conflict Studies, Cornell University and Associate Senior Researcher at the Barcelona Centre for International Affairs (CIDOB).

Salvatore Parente is Researcher in Tax Law in the Department of Economics, Management and Business Law, University of Bari 'Aldo Moro', Italy.

Lorenzo Picarella is a PhD candidate at the University of Milan, Italy.

Rafał Rejmaniak is Assistant Professor in the Department of Historical and Legal Sciences, Theory and Philosophy of Law, and Comparative Law at the Faculty of Law, University of Białystok, Poland.

Dariusz Szostek is Associate Professor in the Department of Civil Law and Civil Procedure at the Faculty of Law and Administration, Opole University, Poland, Head of the Centre for Legal Problems of Technical Issues and New Technologies; European Parliament AI Observatory science expert (2020–2024), and member of European Union Intellectual Property Office, Chairman of the Scientific Council of the Virtual Department of Law and Ethics.

Adam Wiśniewski is Associate Professor and Head of the Department of Public International Law in the Faculty of Law and Administration, University of Gdańsk, Poland.