Izabela Marcinkowska

ARTIFICIAL INTELLIGENCE AND PROTECTION OF SPACE-BASED DATA

Abstract: Nowadays, artificial intelligence is more and more used. Its application for scientific, commercial and strategic purposes on Earth and outer space raises various legal and ethical issues. It has been developed, among others, to enable processing vast amounts of data by self-learning and adapting to ever-changing circumstances[1]. Artificial intelligence is increasingly used in so-called space-based data from meteorological satellites, telecommunications, Earth observation and satellite navigation. However, the main area in this regard is remote sensing[2]. The data types obtained by remote sensing and their sources may vary, including radio signals or light detection (RADAR or LIDAR, respectively), optical images from the air, and thermal or hyperspectral images. The remote sensing technology and the presence of satellites in space collecting enormous amounts of data have led to the generation of large space data sets ("space big data")[3]. Artificial intelligence in this area makes it possible to collect and analyse giant data sets and thus obtain valuable information, for example, in tracking the migration of people and animal populations, poaching, monitoring land or natural disasters, and water and environmental resources. The use of artificial intelligence, including machine learning, in that field helps scientists to analyse massive data sets faster and more effectively. This article will briefly present the general issues related to artificial intelligence, ethical considerations regarding its application in light of human rights under European law, and the application of EU data protection rules to the so-called space-based data.

Keywords: artificial intelligence, machine learning, Internet of Things, Space-based data protection

[1] L. Soroka, K. Kurkova, *Artificial Intelligence and Space Technologies: Legal, Ethical and Technological Issues*, Advanced Space Law, Volume 3, 2019, pp. 131–132.

[2] Under UN General Assembly Resolution 41/65 Principles relating to remote sensing of the EarthEarth from outer space: "The term 'remote sensing' means the sensing of the Earth's Surface from space by making use of the properties of electromagnetic waves emitted, reflected or diffracted by the sensed objects, to improve the natural resources management, land use and the protection of the environment".

[3] S. Bu-Pasha, H. Kuusniemi, *Data protection and space: What challenges will General Data Protection Regulation face when dealing with space-based data?* (in:) Journal of Data Protection and Privacy, vol. 4, 1, p. 53.

1. GENERAL CONSIDERATIONS REGARDING ARTIFICIAL INTELLIGENCE

Artificial intelligence algorithms enable automatic image processing, detection of targets on satellite images, or the extraction of objects in such pictures, and detection of changes or anomalies, for example, environmental ones, to prevent natural disasters[4]. The use of artificial intelligence in data processing is increasingly important and, in the future, will bring many benefits to science and humanity. However, the collection of vast amounts of data and constant observation of the EarthEarth by satellites, as well as devices using artificial intelligence, are associated with risks related, among other things, to privacy, data protection and human rights, taking into account the fact that the latest technological developments used in the satellite industry, including high-definition remote sensing, the Internet of Things (IoT), global navigation satellite systems (GNSS), or radio communications and 5G networks, can collect data and accurate information, including personal data[5].

For centuries, man has strived to create a thinking creature. For example, the myth of Pygmalion, who created Galatea and requested Aphrodite to breathe life into her, or Hephaestus, who fashioned Pandora out of clay, comes to mind[6]. Creating a quasi-human robot controlled by artificial intelligence has become a reality today[7]. Therefore, many new challenges and dilemmas, both ethical and legal, have arisen[8]. Artificial intelligence has become the subject of interest for computer scientists, mathematicians, sociologists, lawyers and philosophers[9]. We shall wait and see whether artificial intelligence proves to be salvation for humanity, or on the contrary, the increasingly widespread reliance thereon becomes the opening of Pandora's box that will bring danger to the world. Before our eyes, the development of artificial intelligence is taking place so rapidly that even its creators themselves are sounding the alarm.

[4] See more at: https://ts2.space/pl/sztuczna-inteligencja-i-przyszłość-aplikacji-do-teledetekcji-satelitarnej/ access:22.08.2023.

[5] See more in S. Bu-Pasha, H. Kuusniemi, *Data protection and space…* p. 53.

[6] W. Kopaliński*, Słownik mitów i tradycji kultury*, Państwowy Instytut Wydawniczy, Warsaw 1985, p. 872 and 951 respectively. See also L. Soroka, K. Kurkova, *Artificial Intelligence and Space Technologies…* p. 132.

[7] K. Kornacki, M.Stępień, Blade Runner. O prawach quasi-człowieka, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2021, ed. K. Zeidler, *passim.*

[8] See more in: M. Maternowska, *Dylematy odpowiedzialności za roboty sterowane sztuczną inteligencją* (in:) *Nowoczesne Systemy Zarządzania Instytut Organizacji i Zarządzania*/Modern Management Systems Institute of Organization and Management, Volume 17 (2022), No. 3 (July-September) as well as *Prawo w erze sztucznej inteligencji. Cyfryzacja i autonomizacja życia publicznego*, ed. Z. Brodecki and M. Nowicka, Wyższa Szkoła Administracji i Biznesu im. E. Kwiatkowskiego w Gdyni, Gdynia-Pelplin 2023, *passim.*

[9] See. e.g. N. Rajakishore, *Philosophy of Artificial Intelligence: A Critique of the Mechanistic Theory of Mind*, Universal Publishers, Boca Raton, Florida, USA, 2009.

The term artificial intelligence has been coined by John McCarthy, a computer scientist. According to his proposed definition: "It is the science and engineering of making intelligent machines, brilliant computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to biologically observable methods"[10]. Mariola Więckowska, in her paper on artificial intelligence, machine learning, deep learning and GDPR, emphasises that artificial intelligence programs do not analyse data in a traditional, linear way but learn based on processed data, and the results obtained in this way are used for further analysis. The ability to learn, plan, or anticipate makes a machine mimic human behaviour[11].

It seems, therefore, that they are those properties and not the "humanoid" outer shell of the robot, which brings the machine closer to humans. The European Parliament's website distinguishes two types of artificial intelligence: firstly, artificial intelligence "embodied" in the form of robots and autonomous vehicles, drones, as well as the Internet of Things and secondly, software. In the latter case, Internet search engines, speech or face recognition could serve as examples[12]. Thus, artificial intelligence has accompanied us for a long time in everyday life and is present in the devices we use every day, for example, in smartphones, when making online purchases, or when using machine translation or automatic generation of subtitles.

According to the European Commission Communication "Artificial Intelligence for Europe: Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems), or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)"[13].

The above definitions of artificial intelligence refer to intelligent behaviour and decision-making processes. Thus, what is intelligent behaviour or intelligence itself? Aleksander Chłopecki argues that the term intelligence belongs to the sphere of psychology but draws attention to the aspect of self-awareness and data processing, stating that: "intelligence is a certain quantifiable property

[10] What is AI?/Basic Questions (stanford.edu) access:22.08.2023 at www. jmc.standford.edu/artificial-intelligence/what-is-ai/index.html.

[11] M. Więckowska *Artificial Intelligence, Machine Learning, Deep Learning, etyka i RODO - jak to wszystko połączyć* (in:) *Prawo sztucznej inteligencji i nowych technologii 2*, ed. B. Fischer, A. Pązik, M. Świerczyński, Wolters Kluwer, Warsaw 2022, p. 245.

[12] https://www.europarl.europa.eu/news/pl/headlines/society/20200827STO85804/sztuczna-inteligencja-co-to-jest-i-jakie-ma-zastosowania; (access:22.08.2023).

[13] See more: Communication from the Commission, Artificial Intelligence for Europe *{SWD (2018) 137 final}* Brussels, 25.4.2018 COM(2018) 237 final, access: 22.08.2023 at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0237.

relating to the realm of data processing (and consequently reactions leading to desired homeostasis with the outside world) that may or may not be related to self-awareness"[14]. When distinguishing weak and robust artificial intelligence, the author raises the point that recognising artificial intelligence as a simulation of human intelligence and decision-making processes refers to weak artificial intelligence. In such a dichotomous division, weak artificial intelligence means artificial intelligence, which works autonomously thanks to algorithms that enable independent learning. Any possible human control is minimal and usually takes place *ex-post*. On the other hand, artificial solid intelligence is characterised by self-cognitive abilities. In addition, the author presents another division applied in the literature on the subject, namely, the division into narrow, general and superintelligence, i.e. artificial intelligence corresponding to weak artificial intelligence, artificial intelligence that equals human and, finally, artificial intelligence that exceeds human abilities[15].

2. ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS

The decision-making process and the application of algorithms is an essential aspect of the operation of artificial intelligence and data processing. Algorithms exist "in a global data ecosystem", and the output obtained from that place can, in turn, be used as input in subsequent algorithm-based processes. Taking into account the increasing impact of AI and machine learning algorithms on society and the use of these tools to make decisions affecting an individual, human rights concerns have arisen[16]. That aspect is highlighted by the study "Algorithms and Human Rights" on specific aspects of human rights in automated data processing techniques, with particular emphasis on algorithms[17]. It relates to automation, i.e., replacing humans with automated computing systems that enable large-scale data processing, characterised by the speed and number of decisions made, potentially burdened with a lower error rate than the decisions made by humans.

The automated decision-making process based on algorithms is challenging to predict for humans. Algorithms are adaptable and "learn" using data sets to

[14] A. Chłopecki, *Sztuczna inteligencja – szkice prawnicze i futurologiczne,* Monografie Prawnicze Beck, the 2nd edition, Warsaw 2021, p. 2. (unofficial translation).

[15] Ibidem, p. 2–5.

[16] See. L. McGregor, D. Murray and V. Ng, International Human Rights Law as a Framework for Algorithmic Accountability (in:) International and Comparative Law Quarterly, published online by Cambridge University Press, 2019, p. 309–310. access:22.08.2023 at international-human-rights-law-as-a-framework-for-algorithmic-accountability (2).pdf.

[17] Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications prepared by the committee of experts on internet intermediaries (MSI-NET) Council of Europe study DGI (2017) 12; access 22.08.2023 at: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

create new decision-making patterns based on machine learning techniques. Algorithms are able not only to make decisions but also to predict future events. Thus, it is essential that decisions made in an automated manner are impartial and non-discriminatory. It should be remembered that human decision-making processes make it possible to consider exceptional cases or any potential deviations from a rule. Therefore, the role of human rights in relation to algorithms, data processing and decision-making processes is essential. Given that automated decision-making involves algorithm-based analysis and the data sets used for that purpose, both of those elements should be considered when assessing their impact on human rights since, for example, a lack of impartiality in decision-making may involve the algorithm and the database itself.

The study argues that the most heated debate regarding algorithms, automated data processing and human rights relates to the right to privacy since algorithms make it possible to collect, process and use vast amounts of data. For example, it mentions the role of cookies, applications enabling the determination of user preferences, profiling and online tracking applications used in so-called behavioural advertising, or the collection of behavioural data by mobile devices. Data collection may affect human rights, referred to by legal acts of the Council of Europe, and in particular, the right to privacy. Article 8 of the European Convention on Human Rights provides that: "everyone has the right to respect his private and family life, his home and his correspondence"[18]. In addition, the purpose of the Council of Europe Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data: "is to secure [...] for every individual, [...] respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")"[19].

Moreover, threats to human rights are highlighted by the recommendations and declarations of the Council of Europe. For example, Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems introduces a definition of "algorithmic systems", which: "are understood as applications that, often using mathematical optimisation techniques, perform one or more tasks such as gathering, combining, cleaning, sorting, classifying and inferring data, as well as selection, prioritisation, the making of recommendations and decision making [...]"[20].

[18] Article 8 (1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, signed at Rome on 4 November 1950, as amended by Protocols Nos. 11, 14 and 15 supplemented by Protocols Nos. 1,4,6,7,12,13 and 16 available at https://www.echr.coe.int/documents/d/echr/convention_eng

[19] Article 1 of Convention for the Protection of Individuals with regard to Autonomic Processing of Personal Data, Strasburg 28/01/1981 European Treaty Series No. 108. Council of Europe.

[20] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies); See: Appendix to Recommen-

Analysis of large data sets using algorithms enables the system's improved performance and services, for example, in transportation and logistics or medicine, particularly in medical diagnostics. Nevertheless, Recommendation CM/Rec (2020)1 points out that the increasing reliance on algorithmic systems may impact human rights, including the right to privacy and data protection.

Accordingly, it provides guidelines to States as well as to both public and private sector actors on their actions regarding algorithmic systems in their design, development and deployment to ensure the protection of human rights and fundamental freedoms for all individuals as enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms and other relevant treaties. According to the guidelines, member States of the Council of Europe: "shall refrain from violating human rights through the use of algorithmic systems, and shall develop legislative and regulatory frameworks that foster an environment where all actors respect and promote human rights and seek to prevent possible infringements"[21].

In addition, the Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes draws attention to the emergence of new risks related to the aggregation of "constantly expanding volumes of aggregated data on the exercise of human rights". Those risks go beyond the current aspects of privacy and personal data protection. Data optimisation makes it possible to prioritise some values over others, thus affecting the context and environment of information processing by their users and other people and the decision-making processes. The application of machine learning tools is capable not only of predicting the choices made by individuals but also of influencing their emotions and thoughts, sometimes subliminally. This may result in manipulation and control not only in relation to the economic choices of individuals but also their social and even political behaviour, which may pose a threat to democracy due to the significant power that technological progress confers to both public entities and private actors using algorithmic tools without adequate democratic control, or oversight[22].

Advocate General Pitruzzella has drawn attention to the risks associated with gathering, processing and analysing data for a democratic society in the opinion delivered on 27 January 2022 on C817/19 *Ligue des droits humains* versus *Conseil des ministres* regarding the questions referred to the Court of

dation CM/Rec(2020)1: Guidelines on addressing the human rights impacts of algorithmic systems; A. Scope and context, item 2; access: 22.08.2023 at https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

[21] *Ibidem*, item 1.

[22] Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes (Adopted by the Committee of Ministers on 13 February 2019 at the 1337th meeting of the Ministers' Deputies)*;* items 7–8 access: 22.08.2023 at https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b.

Justice of the European Union for a preliminary ruling[23]. It has been argued therein that: the questions on which the Court is required to rule in this case embody one of the principal dilemmas of contemporary liberal democratic constitutionalism: what balance should be struck between the individual and society in this data age in which digital technologies enabled vast amounts of personal data to be collected, retained, processed and analysed for predictive purposes? The algorithms, extensive data analysis, and artificial intelligence used by public authorities can further and protect society's fundamental interests to a hitherto unimaginable degree of effectiveness – from protecting public health to environmental sustainability, from combating terrorism to preventing crime, and serious crime in particular.

At the same time, the indiscriminate collection of personal data and the use of digital technologies by public authorities may give rise to a digital panopticon – where public authorities can be all-seeing without being seen – an omniscient power able to oversee and predict the behaviour of every person and take the necessary measures, to the point of the paradoxical outcome imagined by Steven Spielberg in the film *Minority Report*, where the perpetrator of a crime that has not yet been committed is deprived of his liberty. It is well known that in some countries, society takes precedence over the individual, and using personal data legitimately enables effective mass surveillance aimed at protecting what are considered fundamental public interests. In contrast, European constitutionalism, whether national or supranational, in which the individual and the individual's liberties hold centre stage, imposes a significant obstacle to the advent of a mass surveillance society, especially now that the protection of privacy and personal data have been recognised as fundamental rights. To what extent, however, can that obstacle be set up without seriously undermining specific fundamental interests of society – such as those cited above – which may nevertheless be bound up with the Constitution?

This is at the heart of the digital age's relationship between the individual and society. That relationship, on the one hand, calls for delicate balancing acts between the interests of society and the rights of individuals, premised on the

[23] Cour constitutionnelle (the Belgian Constitutional Court) referred several questions to the Court of Justice of the European Union for a preliminary ruling regarding the interpretation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119, p.1; 'the GDPR'), and Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L119, p.132; ‘the PNR Directive) and its validity as well as Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data. The questions have been referred to in the context of a complaint of the Ligue des droits humains for annulment of the law on processing passenger data.

paramount importance of the individual in the European constitutional tradition, and, on the other, makes it necessary to establish safeguards against abuse. Here, too, we have a contemporary twist on a classic theme of constitutionalism since, as *The Federalist* categorically asserted, men are not angels, which is why legal mechanisms are needed to constrain and monitor public authorities[24].

The quoted passage from the opinion emphasises the role of fundamental rights in protecting private life and personal data. Fundamental rights are a sort of point of reference, guideline and a source of inspiration for the creation of ethical standards for artificial intelligence, which can contribute to the development of a fair democratic society and the well-being of its members. According to the Communication from the Commission "Building Trust in Human-Centric Artificial Intelligence", which provides ethical guidance for trustworthy AI: "AI applications should empower citizens and respect their fundamental rights. They should aim to enhance people's abilities, not replace them […]"[25]. According to "Ethics guidelines for trustworthy AI" developed by the Independent High-Level Group on Artificial Intelligence set up by the European Commission in 2018 (hereinafter referred to as "Ethics Guidelines"), to achieve "trustworthy AI", it is essential that it is lawful (complies with applicable laws and regulations), ethical (developed with respect for ethical principles) as well as robust both from the technical and social perspective. Based on those elements and the values of the Union, the requirements for trustworthy AI have been developed. They include, alongside human agency and oversight, technical robustness and safety, transparency, diversity, non-discrimination and fairness, societal and environmental well-being and accountability, and privacy and data governance.

Ethics Guidelines provide that AI systems can impact fundamental rights, enabling and hampering them. For example, they can help monitor personal data. However, these rights may also be adversely affected. Therefore, assessing the impact on fundamental rights where risks arise *is essential.* According to the Ethics Guidelines, a risk assessment should be *conducted* before developing relevant systems. Moreover, it is necessary to analyse the risks and evaluate whether the risk in question can be avoided, whether it is possible to reduce it or whether any possible risk can be justified to respect the rights and freedoms of others in a democratic society. In addition, the Ethics Guidelines concerned call for the introduction of external feedback systems for AI systems, which

[24] Opinion of Advocate General Pitruzzella delivered on 27 January 2022 in case C817/19 *Ligue des droits humains versus Conseil des ministres,* point 2; access: 22.08.2023 at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62019CC0817.

[25] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Building Trust in Human-Centric Artificial Intelligence Brussels, 8.4.2019 COM(2019) 168 final; access: 22.08.2023 at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0168.

could potentially infringe on fundamental rights[26]. The principle of respect for human autonomy should guide the decision-making process. The Ethics Guidelines base trustworthy AI on fundamental rights and ethical principles. The approach to ethics advocated in that document is based on fundamental rights, which are enshrined in the EU Charter of Fundamental Rights[27], as well as in international human rights law.

The common source of fundamental rights can be found in "respect for human dignity", which presupposes an intrinsic value of every human being. New technologies like artificial intelligence must not be limited or infringed upon. Man cannot be an object; what is essential is that humans are moral subjects[28]. Ethics Guidelines emphasise the importance of a "human-centric approach"[29]. Under the document mentioned above: "Understood as legally enforceable rights, fundamental rights, therefore, fall under the first component of Trustworthy AI (lawful AI), which safeguards compliance with the law. Understood as the rights of everyone, rooted in the inherent moral status of human beings, they also underpin the second component of Trustworthy AI (ethical AI), dealing with ethical norms that are not necessarily legally binding yet crucial to ensure trustworthiness"[30]. The document concerned raises the importance of respect for human dignity, freedom of the individual, democracy, justice and the rule of law (among others, ensuring due process and equality before the law), equality, non-discrimination and solidarity, as well as citizens' rights (including the right to good administration).

As mentioned before, fundamental rights have inspired the development of an ethical framework for AI. The Ethics Guidelines list four ethical principles that are linked to fundamental rights, namely: respect for human autonomy (that is associated with the right to human dignity and liberty)[31], prevention of harm (which is linked to the protection of physical or mental integrity)[32],

[26] Independent High-Level Group on Artificial Intelligence set up by the European Commission "Ethics Guidelines for Trustworthy AI" ("Ethics Guidelines") access: 22.08.2023 at file:///C:/Users/oem/Downloads/ai_hleg_ethics_guidelines_for_trustworthy_ai-en_87F84A41-A6E8-F38C-BFF661481B40077B_60419.pdf

[27] Charter of Fundamental Rights of the European Union (2012/C 326/02) Official Journal of the European Union C 326/391 of 26.10.2012 ("the Charter").

[28] See: "Ethics Guidelines"…, p. 10.

[29] See also Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Building Trust in Human-Centric Artificial Intelligence Brussels, 08.04.2019 COM(2019) 168 final which refers, among other things, to ethics guidelines for trustworthy AI.

[30] See: "Ethics Guidelines"…, pp. 10–12.

[31] Under Article 1 of the Charter: "Human dignity is inviolable. It must be respected and protected according to Article 6 of the Charter: "Everyone has the right to liberty and security of person."

[32] Pursuant to Article 3 of the Charter: "Everyone has the right to respect for his or her physical and mental integrity".

fairness (which is related to the rights to non-discrimination, solidarity and justice)[33], as well as the principle of explicability (that is associated with responsibility and linked to the rights relating to justice[34]). In privacy protection and data governance, Ethics Guidelines combine privacy, a fundamental right affected explicitly by AI systems, with the principle of harm prevention. Adequate data governance is essential to prevent privacy harm. This includes the quality and integrity of the data, access to data and the capability to process it in such a way as to ensure the protection of privacy[35].

Privacy protection[36] Artificial intelligence systems are required throughout the so-called life cycle. This applies not only to the input data provided by users but also to the data generated by the system since artificial intelligence systems will have digital records of human behaviour, allowing to infer individuals' preferences, age, gender, sexual orientation, or even religious and political views. In order to maintain user trust, data mustn't be used unfairly, unlawfully or in a discriminatory manner. In addition, from the point of view of data protection, its integrity and quality are essential, since data may contain errors or social biases. Not only the use of data but also the artificial intelligence systems themselves should be fair. The Ethics Guidelines indicate two dimensions of fairness, i.e. the substantive dimension and the procedural one. Regarding the substantive dimension, an equal and fair distribution of costs and benefits to avoid discrimination, unfair bias and even stigmatisation of individuals or groups of people is referred to.

In the light of the principle of fairness, equal opportunity should be promoted regarding access not only to technology but also to goods, services and education. Systems must not have the effect of deceiving users or interfering with their freedom of choice. What is more, in the light of the principle of fairness, the principle of proportionality ("proportionality between means and ends") must be respected; that is to say, measures should be adapted to the objectives and those which are the least adverse to fundamental rights and ethical norms should be selected. On the other hand, procedural fairness entails contesting decisions taken by artificial intelligence systems and humans who operate them and effectively seeking redress. However, for this to be achievable, it must be possible to identify the respective entities and explain the relevant decision-making processes[37].

[33] Article 21 of the Charter prohibits any discrimination based in particular on sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation, or on grounds of nationality.

[34] Article 47 of the Charter ensures the right to an effective remedy and a fair trial.

[35] See: "Ethics Guidelines"..., pp. 17–18.

[36] Article 7 of the Charter states, "Everyone has the right to respect for his or her private and family life, home and communications".

[37] See: "Ethics Guidelines"..., pp. 12–13.

The principle of explicability is essential for the users' trust in AI systems. According to the principle in question, both the objectives and capabilities of these systems should be communicated openly, and the respective processes should be transparent. Moreover, the decisions taken also require transparency. It should be possible to explain to those affected, directly or indirectly, why a given model that had been used resulted in a particular decision or a specific outcome. In addition, it should explain what input factors have been the basis of a particular decision. Otherwise, the so-called "black box" algorithms could occur[38].

In addition, ethical issues and the importance of fundamental rights, including respect for dignity, are referred to in the Resolution with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies[39] which, among others, relates to respect for privacy, restrictions on the use of biometrics, and the right to seek redress. Pursuant to Article 5 of the Proposal for a Regulation of the European Parliament and of the Council on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies annexed to the Resolution concerned, entitled "Ethical principles of artificial intelligence, robotics and related technologies": "Any artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced by such technologies, shall be developed, deployed and used in the Union in accordance with Union law and in full respect of human dignity, autonomy and safety and other fundamental rights set out in the Charter".

Regarding respect for privacy and personal data protection, Article 12 draws attention to the particular risk to fundamental rights associated with collecting biometric data or facial recognition. They may only be used by the public authorities of the Member States for substantial public interest purposes, and their application requires public disclosure, must be proportionate, targeted, time-restricted and shall be limited to specific locations and objectives. Above all, however, the above must comply with Union and national law and consider human dignity, autonomy and fundamental rights, as laid down in the Charter of Fundamental Rights, with particular regard to the right to respect for privacy and the protection of personal data. Article 13 relates to the right to redress. According to the provision quoted: "Any natural or legal person shall have the right to seek redress for injury or harm caused by the development, deployment and use of high-risk artificial intelligence, robotics and related technologies, including software, algorithms and data used or produced

[38] Ibidem, p. 13.

[39] 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)) access: 22.08.2023 at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html.

by such technologies, in breach of Union law and the obligations set out in this Regulation”[40].

Zbigniew Pinkalski notes that this is only an expression of the general will and, similarly to the Act on Artificial Intelligence, it does not contain any specific solutions with regard to the procedural aspects of liability for the operation of artificial intelligence systems[41]. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) – aims to establish a uniform legal framework for AI in conformity with Union values as regards the development, marketing and use of AI[42]. The Preamble stresses the importance of uniform Regulation relating to the use of AI for legal certainty purposes since the introduction by individual Member States of their own national rules to ensure compliance with fundamental rights obligations would foster fragmentation of both the rules and the internal market.

The Preamble raises that the legal basis in that respect is included in the Treaty on the Functioning of the European Union (TFEU)[43] *inter alia* with regard to the processing of personal data. Pursuant to the second recital: “To the extent that […] Regulation contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for ‘real-time’ remote biometric identification[44] In pub-

[40] The proposed Regulation provides for issuing a European certificate of ethical compliance by the relevant national supervisory authority following a positive assessment of the conformity of artificial intelligence with ethical principles. See art. 16 thereof.

[41] Z. Pinkalski, Sądowe dochodzenie roszczeń związanych z działaniami sztucznej inteligencji – problem dla sądownictwa czy problem legislacyjny? (in:) Prawo sztucznej inteligencji i nowych technologii…pp. 298–299.

[42] See recital 1 of the Preamble to the 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 {SEC(2021) 167 final} – {SWD(2021) 84 final} – {SWD(2021) 85 final}* access: 22.08.2023 at eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

[43] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) Official Journal of the European Union C 202/1 of 07.06.2016.

[44] Pursuant to Article 3 (33) of the Regulation: “ ‘[b]iometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data” and pursuant to recital 8: “The notion of remote biometric identification system as used in […] Regulation should be defined functionally, as an AI system intended for the identification of natural persons at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used. Considering their different characteristics and manners in which they are used and the risks involved, a distinction should be made between 'real-time' and 'post' remote biometric identification systems. In the case of 'real-time' systems, the capturing of the biometric data, the comparison, and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. […]”.

licly accessible spaces for the purpose of law enforcement, it is appropriate to base this Regulation, in as far as those specific rules are concerned, on Article 16 of the TFEU"[45]. Furthermore, it is appropriate to consult the European Data Protection Board[46]. The proposal for a Regulation (Artificial Intelligence Act) contains a catalogue of prohibited AI practices, including the use of real-time remote biometric identification systems in public spaces for law enforcement purposes unless the exceptions indicated in the Regulation are applicable[47].

Article 10 of the Regulation on data and data governance relates to high-risk artificial intelligence systems. Pursuant to Article 10 (5): "to the extent that it is strictly necessary for ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued"[48].

The fundamental rights protected by the Charter of Fundamental Rights are the benchmark for classifying AI systems as high-risk. According to Recital 27 of the Preamble, "[…] AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union […]". This is confirmed by Recital 28, according to which: "[…] The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk. These rights include, *inter alia*, the right to human dignity, respect for private and family life and the protection of personal data. The Explanatory Memorandum to the proposal for the Regulation, with regard to fundamental rights, provides that the use of artificial intelligence may adversely affect fundamental rights enshrined in the EU Charter of Fundamental Rights".

The proposal aims to protect these rights and identify sources of risk based on a risk analysis. The requirements for artificial intelligence and the obliga-

[45] Article 16 TFEU provides that: "1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities".

[46] See the second recital of the Regulation.

[47] See Art. 5 of the Regulation.

[48] Article 10 (5) of the Regulation

tions of the value chain's participants are intended to contribute to the protection of fundamental rights enshrined in the Charter, such as *inter alia*, the right to human dignity (Article 1 of the Charter), respect for private life and protection of personal data (Articles 7 and 8 of the Charter). Due to the introduction of *ex-ante* testing and other human oversight as well as risk management obligations, it will be possible to minimise possible erroneous or biased decisions made by artificial intelligence. On the other hand, *ex-post* controls and the transparency and traceability of AI systems will enable effective redress for persons whose fundamental rights have been infringed[49].

The solutions provided for in the Regulation (the Artificial Intelligence Act) are vital, among others, from the point of view of due process (procedural fairness). However, it is argued in the literature that it is necessary to provide more details with regard to any possibility of redress by individuals[50]. Nevertheless, first of all, as the Commission Communication – Building Trust in Human-Centric Artificial Intelligence highlights, it should be taken into account that: "[…] trust is a prerequisite to ensure a human-centric approach to AI: AI is not an end in itself, but a tool that has to serve people with the ultimate aim of increasing human well-being. To achieve this, the trustworthiness of AI should be ensured. The values on which our societies are based need to be fully integrated into the way AI develops. The Union is founded on respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities […]"[51].

3. SPACE-BASED DATA PROTECTION

Academic writings combine issues related to artificial intelligence and ethics with the right to privacy and personal data protection. As regards satellite data that is collected and disseminated mainly by remote sensing, the INSPIRE Directive applies[52]. However, in general, it addresses spatial data and environmental issues. As far as the protection of personal data and privacy is con-

[49] See item 3.5. of the Explanatory Memorandum to the Regulation entitled: "Fundamental rights".

[50] Z. Pinkalski proposes relevant solutions in that respect. See: Sądowe dochodzenie roszczeń…, pp. 301–304.

[51] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Building Trust in Human-Centric Artificial Intelligence Brussels, 08.04.2019 COM(2019) 168 final, p. 1–2; access 22.08.2023 at https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence

[52] Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), Official Journal of the European Union L 108/1 of 25.04.2007.

cerned, the leading legal act under EU law, namely, the General Data Protection Regulation (hereinafter referred to as "GDPR")[53] is applicable. Some scholars promote a narrow interpretation of GDPR and argue that the GDPR Regulation only protects personal data. However, others, such as Hielke Hijmans and Charles Raab[54] claim that GDPR has an ethical dimension. Thus, it constitutes a normative framework based on values, including, *inter alia*, fundamental rights and principles[55].

Regarding satellite-based data in the context of data protection, particularly the GDPR, the applicability of that Regulation to satellite-based data should be examined. Although satellites move in outer space, their boundaries could be more precise. A. Szpak provides a few concepts. As far as the first one is concerned, which is based on the layers of the atmosphere (i.e. troposphere, stratosphere, mesosphere, ionosphere and finally the exosphere), outer space begins at about 100 km from the Earth's surface due to the composition of the atmosphere. According to the second concept, the boundary between airspace and outer space is based on the technical operation of aircraft. Finally, according to the third concept, airspace spreads as far as the possibilities of exercising the power and exploitation of outer space by the States. In other words, airspace could extend as far as the States could extend their sovereignty.

However, the author emphasised that nowadays, that theory could not be accepted due to the prohibition on appropriating outer space and celestial bodies[56]. *Fédération* Aéronautique Internationale (FAI), an international body responsible for keeping aeronautical records, has set a border, the so-called Kármán line, between airspace and outer space at an altitude of 100 kilometres above the Earth's surface[57], which seems to be consistent with the first of the concepts presented. As it has been mentioned above, the prohibition of appropriation of both the outer-space and celestial bodies should be taken into ac-

[53] 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, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1 of 04.05.2016 ("GDPR").

[54] H. Hijmans and C. Raab, Ethical Dimensions of the GDPR (in:) M.Cole and F. Boehm (eds.) Commentary on the General Data Protection Regulation, Edward Elgar 2018.

[55] See more in European framework on ethical aspects of artificial intelligence, robotics and related technologies, European added value assessment, Study of the European Parliamentary Research Centre, p. 6.

[56] A. Szpak Prawo kosmiczne w pigułce, Edukacja Prawnicza No. 1 (121) January2011, access 22.08.2023 at https://www.edukacjaprawnicza.pl/prawo-kosmiczne-w-pigulce/ (access: 22.08.2023).

[57] However, NASA sets this boundary at 80 km above the EarthEarth. Gdzie zaczyna się przestrzeń kosmiczna? – National Geographic (national-geographic. pl) See more broadly on the concept of the division into airspace, near space and outer space as well as global data protection legislation https://www.michalsons.com/blog/spacetech-do-data-privacy-laws-apply-to-outer-space/45577 (access: 22.08.2023).

count. Pursuant to Article 1 of the Space Treaty: "The exploration and use of outer space, including the Moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind […]". In addition, according to Article 2 of the Space Treaty: "Outer space, including the Moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means"[58].

However, data processing usually takes place on the Earth. Thus, the GDPR will be applicable, with some exceptions, to data transmitted via satellite and remote sensing when the personal data of EU citizens is taken into account and such data is processed on Earth[59]. Pursuant to art. 4 (2) of GDPR relating to definitions: (2) "'processing' means any operation or set of operations which is performed on personal data[60] or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". It should be noted in this place that in terms of this paper, data obtained by satellites is concerned.

The territorial scope of application of GDPR is determined by Article 3 thereof, which provides: "1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union […]". Therefore, the provisions of GDPR are applicable not only to EU satellite companies but also to non-EU ones if they offer goods and services in the European Union or to the data subjects in the European Union. Thus, in some cases, the Regulation in ques-

[58] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies; (in:) United Nations Treaties and Principles on Outer Space Text of treaties and principles governing the activities of States in the exploration and use of outer space, adopted by the United Nations General Assembly, United Nations, New York, 2002, p. 4.

[59] S. Bu-Pasha, H. Kuusniemi, Data protection and space…, p. 54.

[60] Article 4 (1) GDPR provides: "Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

tion allows for extraterritorial application[61]. GDPR applies, for example, to satellite services and data in connection with telecom services or TV broadcasting when data is gathered and processed by companies and the service providers acting as data processors and controllers. However, it is essential to distinguish whether a satellite operator acts as a controller or a processor in view of their respective obligations[62].

The material scope of GDPR's application is covered by Article 2 thereof. Pursuant to art.2(1): "This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system". Article 2(2) provides for exemptions to the applicability of the Regulation. In addition, attention should be drawn to art. 2(3), which contains a subject-related exemption, namely: "For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. […]". The act referred to in the above provision, namely Regulation (EC) No 45/2001, of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[63] has been replaced by a new one, namely, Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data[64] to meet, among others, the requirements of GDPR for institutions in accordance with the data protection requirements of GDPR.

For example, Article 5 of Regulation 2018/1725 corresponds to Article 6 of GDPR relating to the lawfulness of processing. In many cases, satellite data is processed by EU institutions, and that is not subject to GDPR. In such cases, Regulation 2018/1725 referred to above is applicable. The Copernicus programme, i.e. the Earth observation programme, which produces a lot of data, could serve as an example in this place. The technical side of the program is coordinated by the European Space Agency (ESA). However, the main coordinating and managing actors are the EU institutions, which work in partnership with States[65].

[61] S. Bu-Pasha, H. Kuusniemi, Data protection and space..., p. 55; See also L. Soroka, K.Kurkova, Artificial Intelligence and Space Technologies…, p. 136

[62] S. Bu-Pasha, H. Kuusniemi, Data protection and space…, p. 54.

[63] Official Journal of the European Communities L No. 8 of 12.01.2001, p. 1.

[64] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, Official Journal of the European Union L 295/39 of 21.11.2018.

[65] S. Bu-Pasha, H. Kuusniemi, Data protection and space…, p. 55.

Satellites are often operated by public authorities or States. In some cases, it is possible to limit the application of GDPR[66]. The restrictions may relate to national, public or defence issues[67], Under certain circumstances, unrestricted access to data could compromise security issues. Otherwise, when transparency and open access do not endanger security, if satellite technologies collect the personal data of an individual, the individual should be informed thereof, and the data collected should not exceed the initially intended scope of sharing[68].

Therefore, it is worth considering the issue of free access to space-based data. Shakila Bu-Pasha and Heidi Kuusniemi emphasise that a balance must be struck between legal issues relating to data as well as data ownership and the public interest. They draw attention to two approaches in that respect. On the one hand, the protection of personal data and privacy is recognised as a fundamental human right in the EU, and on the other hand, the free flow of data and platforms of open data are promoted to support business suitability. A similar approach is formulated with regard to space-based data. However, the protection of personal data and the right to privacy must be taken into account when open access to data is concerned. In that respect, it is worth quoting the 4th recital of GDPR[69], according to which: "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not absolute; it must be considered in relation to its function in society and be balanced against other fundamental rights in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity".

CONCLUSION

Given the rapid technological progress and the increasing role of artificial intelligence, which is also used in space activities and data processing, it is crucial to keep in mind the ethical issues and values that should provide guidelines for the development of normative solutions designed for new technologies, respecting human rights and fundamental rights, such as the right to

[66] Ibidem, 56.

[67] Article 23 of the GDPR lists among the restrictions, for example, national or public security.

[68] S. Bu-Pasha, H. Kuusniemi, Data protection and space…, p. 56

[69] Ibidem

privacy as well as the protection of personal data as its aspect. Considering the development of space and artificial intelligence laws, it should be human-oriented, and human rights are to play a leading role in that respect.

BIBLIOGRAPHY

Bu-Pascha: S. Bu-Pasha, H. Kuusniemi, Data protection and space: What challenges will General Data Protection Regulation face when dealing with space-based data? (in:) Journal of Data Protection and Privacy, vol. 4, 1;

Chłopecki: A. Chłopecki, Sztuczna inteligencja – szkice prawnicze i futurologiczne, Monografie Prawnicze Beck, the 2nd edition, Warsaw 2021;

Hijmans: H. Hijmans and C. Raab, Ethical Dimensions of the GDPR (in:) M.Cole and F. Boehm (eds.) Commentary on the General Data Protection Regulation, Edward Elgar 2018;

Kopaliński: W. Kopaliński, Słownik mitów i tradycji kultury, Państwowy Instytut Wydawniczy, Warsaw 1985;

Kornacki: K. Kornacki, M.Stępień, Blade Runner. O prawach quasi-człowieka, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2021, ed. K. Zeidler;

Maternowska: M. Maternowska, Dylematy odpowiedzialności za roboty sterowane sztuczną inteligencją (in:) Nowoczesne Systemy Zarządzania Instytut Organizacji i Zarządzania/Modern Management Systems Institute of Organization and Management, Volume 17 (2022), No. 3;

McGregor: L. McGregor, D. Murray and V. Ng, International Human Rights Law as a Framework for Algorithmic Accountability (in:) International and Comparative Law Quarterly, published online by Cambridge University Press, 2019;

Rajakishore: N. Rajakishore, *Philosophy of Artificial Intelligence: A Critique of the Mechanistic Theory of Mind*, Universal Publishers, Boca Raton, Florida, USA, 2009;

Pinkalski: Z. Pinkalski, Sądowe dochodzenie roszczeń związanych z działaniami sztucznej inteligencji – problem dla sądownictwa czy problem legislacyjny? (in:) Prawo sztucznej inteligencji i nowych technologii 2, ed. B. Fischer, A. Pązik, M. Świerczyński, Wolters Kluwer, Warsaw 2022;

Soroka: L. Soroka, K.Kurkova, Artificial Intelligence and Space Technologies: Legal, Ethical and Technological Issues, Advanced Space Law, Volume 3, 2019;

Szpak: A. Szpak Prawo kosmiczne w pigułce, Edukacja Prawnicza No. 1 (121) January 2011, access 22.08.2023 at https://www.edukacjaprawnicza.pl/prawo-kosmiczne-w-pigulce/;

Więckowska: M. Więckowska Artificial Intelligence, Machine Learning, Deep Learning, etyka i RODO – jak to wszystko połączyć (in:) Prawo sztucznej inteligencji i nowych technologii 2, ed. B. Fischer, A. Pązik, M. Świerczyński, Wolters Kluwer, Warsaw 2022.