ZESZYT PRAWNICZY UAM

NR 15/2025

Wydawnictwo Naukowe UAM

UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

ZESZYT PRAWNICZY UAM

NR 15/2025

WYDAWNICTWO NAUKOWE

POZNAŃ 2025

Zeszyt Prawniczy UAM
(wcześniej Zeszyt Studencki Kół Naukowych Wydziału Prawa i Administracji UAM, ISSN 2299-2774)

Adres redakcji
al. Niepodległości 53, 61-714 Poznań, Collegium Iuridicum Novum, sala W2
e-mail: zeszyt@amu.edu.pl, www.zeszyt.amu.edu.pl

Publikacja sfinansowana przez Wydział Prawa i Administracji
Uniwersytetu im. Adama Mickiewicza w Poznaniu

Wersja pierwotna czasopisma: elektroniczna

Redakcja: *Marzena Urbańczyk*
Redakcja techniczna/DTP: *Reginaldo Cammarano*

ISSN (Online) 2956-2767 ISSN (Print) 2720-2526 DOI: 10.14746/zpuam

WYDAWNICTWO NAUKOWE UNIWERSYTETU IM. ADAMA MICKIEWICZA W POZNANIU
61-701 POZNAŃ, UL. A. FREDRY 10
www.press.amu.edu.pl
Sekretariat: tel. 61 829 46 46, faks 61 829 46 47, e-mail: wydnauk@amu.edu.pl
Dział Promocji i Sprzedaży: tel. 61 829 46 40, e-mail: press@amu.edu.pl

Wydanie I. Ark. wyd. 9,50. Ark. druk. 8,50

DRUK I OPRAWA: VOLUMINA.PL SP. Z O.O., SZCZECIN, UL. KS. WITOLDA 7–9

Contents

ARTICLES

ARTICLES

ZESZYT PRAWNICZY UAM
NR 15/2025
https://doi.org/10.14746/zpuam.2025.15.1

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

SARA DOBOSZ

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0008-3365-3397
sardob3@st.amu.edu.pl

MIKOŁAJ WIDLIŃSKI

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0004-6818-7788
mikwid@st.amu.edu.pl

Social Scoring: Opportunities and Threats for Contemporary Society Using the Example of the People's Republic of China

Abstract: The purpose of this article is to analyse the social assessment system in the context of its potential opportunities and threats, with particular reference to the example of the People's Republic of China. The study is based on an analysis of the literature and legislation governing the use of artificial intelligence systems in the European Union and internationally. The paper outlines the mechanism of the social rating system, its impact on social stratification, and its ethical and legal implications. The analysis also covers the Chinese Social Credit System, its structure, functioning and consequences for citizens, indicating its impact on social and economic life. Conclusions show these systems can deepen inequalities and violate rights, stressing the need for strong regulation.

Keywords: social scoring, AI Act, Social Credit System, China

Introduction

Over recent years, the role of artificial intelligence has grown significantly in many areas of life. While the rapid development of new AI technologies brings many advantages, it also entails numerous risks related to breaches of privacy, and the protection of personal data, as well as potential impacts on citizens' rights and freedoms. In particular, the uncontrolled use of artificial intelligence systems to profile citizens and then to issue automated administrative, business or financial decisions may raise concerns.

The publication focuses on the theoretical underpinnings and functioning of social scoring systems, using the Social Credit System introduced by the government of the People's Republic of China as a case study, and argues that while such systems may improve administrative efficiency and behavioural compliance, they pose serious threats to individual rights, reinforce social inequalities, and raise fundamental ethical and legal concerns.

1. Explanation of the Concept and Mechanism of the Social Scoring System

Social scoring can be defined as an algorithmic regulation system that uses scoring mechanisms to shape collective behaviour through the use of grades as incentives.[1] The premise of the system is to elicit reactions in individuals that are positive from the point of view of the entity that implemented the system. Behaviour categorised as positive boosts a citizen's overall rating, while negative behaviour lowers it. A higher rating facilitates access to goods and services and special privileges, such as a better job, the opportunity to gain an education at the best universities, or obtain credit on preferential terms. A low score, on the other hand, can isolate an individual from the rest of society by limiting access to services reserved for those with higher scores.

The basic mechanics of a social rating system involves each citizen being given a certain initial score, which is then altered through certain actions and behaviours engaged in by the individual. Even at the initial stage, it is possible for a child to be discriminated against and indirectly held responsible for the actions of the parents, as their initial rating may depend on their past activity. In the event that parents have a high rating, their children could already be in a privileged position at the start and receive a higher score.

In addition to monitoring the citizens' behaviour as individuals, a social rating system could also analyse interactions with other people, the social environments in which the individual rotates, his/her habits, customs, preferences. Such a mechanism would serve to create a profile of a person that takes into account his or her lifestyle and level of civic engagement, thus creating a comprehensive picture of the individual in a social context.

2. Social Stratification

Introducing a social rating system can lead to existing social divisions being perpetuated and deepened. According to sociologist Max Weber, the key elements of social stratification are wealth, power and prestige, each of which may be significantly affected by the functioning of such systems.

Wealth plays a crucial role in determining an individual's access to opportunities. Individuals originating from families with low social scores may encounter barriers in accessing high-quality education and elite universities. Limited educational opportunities, in turn, reduce their chances of obtaining well-paid employment, which perpetuates lower income levels and restricts upward mobility. Conversely,

[1] Nello Cristianini and Teresa Scantamburlo, "On Social Machines for Algorithmic Regulation," *AI & Society: Knowledge, Culture and Communication* 35, 2020: 651.

those with higher social ratings benefit from preferential access to prestigious institutions and career advancement, which further consolidates their privileged position—sometimes reinforced through activities such as philanthropy, which positively affect their scores.

Power is also shaped by social rating mechanisms. Individuals who receive negative evaluations may be excluded from leadership roles and decision-making positions. As a result, political, administrative and organisational influence remains concentrated among those who established or uphold the rules of the scoring system. This dynamic reinforces existing hierarchies and limits democratic access to positions of authority.

Prestige, understood as social recognition and respect, may become increasingly tied to one's social score. Evaluation systems contribute to the stigmatisation of low-rated individuals, whose social interactions can negatively impact the ratings of others, leading to their gradual exclusion from public life. In contrast, high scorers enjoy increased recognition and trust, often based not only on personal merit but also on inherited social capital.

As access to resources, power and respect becomes increasingly dependent on algorithmic outcomes, social mobility is gradually being replaced by systemic reinforcement of inherited advantage. Over time, these dynamics are likely to result in the entrenchment of existing inequalities, with the gap between high and low-rated individuals continuing to grow, thus reinforcing systemic social stratification.[2]

3. Potential Risks and Concerns

The introduction of a system of social assessments raises a number of ethical concerns and risks related to both the violation of citizens' fundamental rights and potential socio-economic impacts.

A key issue seems to be issues related to the processing of personal data and the violation of individual privacy. Social assessment systems rely on collecting and analysing large amounts of information about citizens. This data can range from basic information usually collected by public authorities to that related to monitoring an individual's activity in society. This makes the issue of the potential leakage of this data all the more serious, as social assessment systems will collect a comprehensive picture of an individual's activities, combining different sources of information into a single database.

Equally dangerous could be the psychological burden on citizens. The awareness of being constantly monitored and assessed can lead to increased anxiety

[2] "Social Scoring Systems: Current State and Potential Future Implications," Kaspersky Blog, https://www.kaspersky.com/blog/social-scoring-systems/, accessed 10 March 2025.

and people withdrawing from social life. The need to adapt one's behaviour to the expectations of the social evaluation system can result in self-censorship, reduced freedom of expression, and a refusal to take actions that could be negatively evaluated. In the long term, this can lead to social conformity, in which individuals adhere to certain norms not because they are right, but for fear of negative consequences. What emerges is not simply a surveillance apparatus, but a form of quiet governance that rewards submission and penalises deviation, regardless of actual harm or benefit to society.

Moreover, the mechanism of the social evaluation system and the way it is scored can be difficult to understand. Citizens may not have access to full information about the assessment criteria or the specific actions that influenced their score, which would make it difficult to challenge possible errors in the system. With this state of affairs, it is not difficult to be manipulated, both by users who wish to improve their ratings and by private and public institutions that may abuse the system to achieve their own ends. Such a lack of transparency would lead to a deepening sense of injustice and helplessness in the face of the system's arbitrary decisions.

4. Legal Regulations

The dynamic development of artificial intelligence and, at the same time, the resulting risks have been recognised at EU level. This is reflected in Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, which lays down harmonised rules on artificial intelligence and amending Regulations (Artificial Intelligence Act). At the outset, it should be noted that the EU legislator does not provide a clear assessment of what role artificial intelligence plays nowadays, but recognises both its negative and positive aspects in an attempt to ensure the necessary protection of individuals without limiting technological development. The regulation indicates that it aims to improve the functioning of the internal market and promote the spread of human-centred and trustworthy artificial intelligence.[3]

Three key aspects relevant to social assessments can be extracted from the content of the regulation: transparency, non-discrimination and accountability. These safeguards suggest an awareness that non-transparent or biased evaluating systems, such as those based on social scoring, can distort the very idea of fairness that modern democracies seek to uphold:

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024), Recital 1.

– Transparency of systems, linked to Article 22 of the GDPR, refers to the right to obtain an explanation of the outcome of the algorithm. The scope of the algorithm and the mechanics of the system must be understood for high-risk decisions.

– Non-discrimination refers to the need to collect a variety of data in order to avoid bias and prevent uncertain decision-making and unfair use of that data against different groups in society.

– Accountability, on the other hand, relates to the need to identify those responsible for decisions made using artificial intelligence systems.[4]

Pursuant to Article 5(1)(c) of the AI Act, it is prohibited to place on the market, put into service or use AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, where such social scoring leads to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity.[5]

It is important to note that the EU legislator has not chosen to prohibit social assessment systems altogether. The prohibition applies when such assessments lead to unfair or prejudicial treatment in contexts unrelated to the original purpose of the data collection or when such treatment is unjustified or disproportionate to the social behaviour of the person concerned. The doctrine emphasises that the prohibition should not affect the lawful practice of assessing individuals which is carried out for a specific purpose in accordance with Union and national law.[6]

Article 5(1)(h) of the Regulation also prohibits the use of real-time remote biometric identification systems in public spaces for law enforcement purposes, except when their use is strictly necessary for specific purposes, such as searching for victims of abduction, trafficking and sexual exploitation, preventing imminent danger to life or terrorist attacks, and identifying suspects of serious crimes punishable by a prison sentence of at least four years.[7]

In the case of real-time systems, biometric data capture, comparison and identification take place instantly or almost instantly (without major delays). Systems that use surveillance cameras to analyse images in real time and identify citizens

[4] Aviad Raz and Jusaku Minari, „AI-Driven Risk Scores: Should Social Scoring and Polygenic Scores Based on Ethnicity Be Equally Prohibited?" *Frontiers in Genetics* 14, 2023: 1169580, https://doi.org/10.3389/fgene.2023.1169580.

[5] Artificial Intelligence Act, Article 5.

[6] Els J. Kindt and Catherine Jasserand, "Commentary on Article 5. Prohibited AI Practices," in *The EU Artificial Intelligence (AI) Act: A Commentary*, ed. Ceyhun Necati Pehlivan et al. (Wolters Kluwer, 2024), 109.

[7] Artificial Intelligence Act, Article 5(1)(h).

on the basis of these images should therefore fall into this category. In the case of post-factum systems, this provision will not apply, as the biometric data have been captured beforehand and their comparison and identification occur at a later stage. This applies to material such as photographs or video recordings from surveillance cameras or private devices, which were generated before the biometric identification system was used.

In November 2021, the United Nations Educational, Scientific and Cultural Organisation (UNESCO) adopted Recommendations on the Ethics of Artificial Intelligence through a resolution of its 41st General Conference. Among the recommendations is that artificial intelligence systems should not be used for social scoring or the exercise of mass surveillance.[8]

5. Introduction to Social Credit System

For the foreseeable future, nearly one and a half billion citizens of the People's Republic of China (PRC) will be subjected to continuous evaluation under the Social Credit System (SCS). The scope of this endeavour is unprecedented and unmatched by any previous social engineering project in human history.[9]

Initial declarations by the Government of the People's Republic of China envisaged full centralisation of the system by 2020, but this proved unrealistic. In 2022, the Chinese authorities published the first version of regulations that systematised the operation of the Social Credit System, documenting the implementation process to date and setting directions for increasing its effectiveness in the future. Currently, there is no official information on the final date for the full implementation of the system at the national level.

The idea of social engineering is not a new phenomenon in China. The Social Credit System is a development of previous social control mechanisms, but one enriched with advanced data analysis technologies. The foundations of the current concept of social governance were established under the Hu Jintao government (2002–2012) as part of the "small state, big society" strategy. The system therefore does not represent a radical change in the Communist Party of China's (CPC) approach to the governance of society, but rather an evolution in response to global technological change.[10]

---

[8] United Nations Educational, Scientific and Cultural Organization, "Recommendation on the Ethics of Artificial Intelligence," 2022, 20.

[9] Mateusz Bartoszewicz, "Chiński System Zaufania Społecznego," *Przegląd Geopolityczny* 32, 2020: 58–67.

[10] Alicja Bachulska, *Rozwój systemu oceny wiarygodności społecznej w ChRL: między "orwellowskim koszmarem" a technokratyczną utopią?* (Ośrodek Badań Azji, Centrum Badań nad Bezpieczeństwem, Akademia Sztuki Wojennej, 2019).

6. Structure of the Social Credit System

The Social Credit System aims to create mechanisms for rewarding and punishing individuals based on an assessment of their trustworthiness. It consists of three main components: a "blacklist" system, financial credibility rankings and local social rankings.

The first of these mechanisms, the "blacklist" system, is a nationwide register of individuals who have breached existing regulations. These lists are publicly accessible, made available through government websites or posted on local notice boards. Individuals on these lists are subject to a wide range of sanctions, including restrictions on the use of public transport, obtaining credit or employment in the public sector. These restrictions are enforced by the so-called Unified Punishment System.[11]

The second key element of the Social Credit System under discussion are the credibility rankings produced by Chinese financial institutions. Of particular note is the Zhima Credit (Sesame Credit) system, a collaboration between public and private entities. This system is being developed by Ant Financial Group Holding, a company owned by the Alibaba Group. Its main objective is to build users' credit history by analysing their activity on the Alipay app. Thanks to the huge amounts of data being harvested in real time and the use of Big Data-based algorithms, the system generates ranking ratings for all active users.

The last component of the SCS, local social rankings, has been introduced experimentally in more than 40 selected pilot cities. This system, also known as "Social Scoring", involves evaluating the citizens of a city based on points awarded that reflect their behaviour. For actions considered negative, citizens lose points. However, for behaviour judged positive, there is the possibility of regaining them.

This type of social credibility assessment system is the most controversial, due to its strongly normative nature. This type of arrangement may raise concerns about the possibility of manipulation and arbitrariness in assessing aspects of social life that are traditionally not subject to numerical valuation, such as the quality of human relations or activities for the public good. Currently, the implementation and oversight of pilot programmes in this area remains the responsibility of local administrations, primarily at city level. Depending on local circumstances, different urban centres implement evaluation systems differently. For example, Suzhou has an Osmanthus Points system, whereby units are rated on a scale from 0 to 200 points. In contrast, the city of Suqian has implemented the Xichu Points system, in which each individual starts with an initial score of 1,000 points and is then assigned to one of the rating categories ranging from AAA (highest) to D (lowest).[12]

[11] Bartoszewicz, "Chiński System Zaufania Społecznego," 60.

[12] Bachulska, *Rozwój systemu oceny wiarygodności społecznej w ChRL*.

The varied approaches to the design and implementation of social scoring systems indicate the lack of a uniform standard and highlight the significant challenges associated with their potential impact on social structures and individual attitudes.

7. Case Study: Rongcheng City

One of the most advanced Social Credit System pilot programmes was implemented in Rongcheng, located in Shandong province with a population of 650,000. The city has recorded above-average results in implementing the SCS.

In 2014, the local city government issued a series of regulations setting out the rules for the operation of social ranking: *Rongcheng Municipal Regulations for Rewarding or Punishing Individual Citizens Based on Credibility Rating and Rongcheng Citizens' Credibility Rating Standards*. According to the rules set out in the documents, each resident of the city starts with a pool of 1,000 points, which can be added or subtracted depending on their actions. For example, false accusations result in a deduction of 30 points, while participation in charitable activities results in an award of 10 points.

The point grading system is based on a scale from "A" to "D". Model reliability ("AAA") is assigned to individuals who have accumulated more than 1050 points. In contrast, individuals whose score falls below 599 points are given a grade of "D" and are considered unreliable.

Those with an "A" rating are eligible for certain incentive measures. Among the most significant privileges is inclusion on the "red list" of creditworthiness, which is a confirmation of their financial reliability. In addition, these individuals may benefit from priority access to enrolment in educational institutions, basic social benefits, social assistance, as well as preferential employment conditions and career advancement. In addition, they may be subject to limited or completely abolished supervisory and control procedures. In turn, individuals whose score places them in the "D" category are placed on a "blacklist", resulting in public disclosure of information about their low reliability. As a consequence, they may become subject to detailed surveillance and monitoring and lose previously awarded honorary titles. In addition, they may be deprived of government financial support, face restrictions on access to credit, and experience the suspension or cancellation of their professional qualifications.

According to data provided by the local government of Rongcheng City, the introduction of the citizen assessment system in 2018 contributed to a significant decrease in the number of administrative cases. In addition, there was a 22.8% decrease in the number of social conflicts and disputes, as well as a reduction in the rate of non-performing loans at financial institutions. The enforcement rate of court decisions increased by 10% compared to the same period in the previous

year. At the same time, the credibility of public administration and the level of trust between government representatives and citizens improved. The public satisfaction index remained high, not falling below 96%.[13]

8. Control or a New Form of Freedom?

The government of the People's Republic of China's assumptions about the Social Credit System cover a much wider scope than just the Chinese territory. The main objective of the system is to classify and monitor as many citizens and institutions operating in the Chinese market as possible. The implementation of this mechanism may put pressure on individual operators who wish to maintain a high ranking and thus remain competitive in the huge Chinese market. It is worth noting that despite the formal "impersonality" of the rating algorithm, the decision to award a particular ranking remains with the PRC government, which has an overriding legal role.[14]

The functioning of the Social Credit System depends on its wide public acceptance. According to research to date, the level of approval among citizens remains high, especially among representatives of the middle class living in large urban areas.[15] The prevailing perception is that the system expands their freedom, especially in the area of consumption and economic opportunities. From the perspective of the average PRC citizen, the Social Credit System can be seen as a tool to facilitate decision-making by setting unambiguous patterns of behaviour. Through an elaborate structure of rewards and sanctions, users of the system are provided with precise guidelines for actions conducive to maintaining a favourable socio-economic position. In addition, the rankings enable individuals to better monitor the consequences of their decisions. But when everyday actions are filtered through a logic of quantifiable reward, freedom itself risks being reduced to a matter of scorekeeping.

Summary

The social scoring system is based on the collection and analysis of data on citizens in order to influence individuals' behaviour through reward and punishment mechanisms. Its introduction can lead to a widening of social inequalities, limiting access to education, the labour market and prestigious positions for those with low grades, as well as reinforcing divisions in society. In addition, the system risks breaching

[13] Mi Zhang, "Analiza Systemu Oceny Wiarygodności Społecznej z wykorzystaniem teorii Nudge" (Master's thesis, Szkoła Główna Handlowa w Warszawie, 2021).

[14] Bartoszewicz, "Chiński System Zaufania Społecznego," 62–63.

[15] Bachulska, *Rozwój systemu oceny wiarygodności społecznej w ChRL*, 63.

privacy, increasing surveillance and self-censorship, and lacking transparency in the setting of grades and their impact on citizens' lives.

In response to these risks, the European Union introduced the AI Act, which prohibits the use of AI systems for social assessment of individuals if it leads to disproportionate or prejudicial treatment. The regulation further prohibits the use of real-time remote biometric identification systems in public spaces, apart from certain security exceptions. At the international level, UNESCO has issued recommendations emphasising that AI systems should not be used for social scoring or mass surveillance.

The introduction of a social scoring system carries serious risks for individual rights and the social fabric. While EU and international regulations emphasise the need to protect privacy and prevent abuse, the challenge remains to enforce these rules effectively and adapt them to the dynamic development of artificial intelligence.

Assessing the Social Credit System in the People's Republic of China requires adopting a specific perspective. From an internal perspective, encompassing the perception of the Chinese Communist Party, its interests and the cultural conditioning of Chinese society, the SCS appears as a natural continuation of existing trends and an effective management and control tool. In contrast, the external perspective, in particular as represented by Western countries considered democratic, highlights significant divergences in the understanding of individual freedom, its relationship with the state or civil rights.[16]

It should be noted that the PRC does not have a unified, nationwide SCS system, but only about a collection of systems that often differ in terms of scoring, assessment methods and the aspects of civic life they influence. The common elements that dominate the Social Credit System are three key areas: the public classification of individuals into "red" and "black" lists, local social rankings and the assessment of the trustworthiness of financial institutions. As time goes on, the number of issues to be analysed and algorithmised is bound to increase. An important milestone in the development of this system is its planned unification and centralisation, covering the entire PRC territory.

Given the growing complexity of the system and China's importance in the global economy, the possibility of adapting selected mechanisms of the SCS outside the country should be considered. However, in light of the risks to individual rights, social equality, and legal safeguards identified throughout this analysis, it remains uncertain whether democratic states would be willing to reconcile such systems with the fundamental principles of their political and legal cultures. The further evolution and long-term consequences of social scoring thus remain a subject of ongoing debate, raising essential questions about the balance between technological efficiency and the preservation of civil liberties.

[16] Bachulska, *Rozwój systemu oceny wiarygodności społecznej w ChRL*, 64.

BIBLIOGRAPHY

Bachulska, Alicja. *Rozwój systemu oceny wiarygodności społecznej w ChRL: między "orwellowskim koszmarem" a technokratyczną utopią?* Ośrodek Badań Azji, Centrum Badań nad Bezpieczeństwem, Akademia Sztuki Wojennej, 2019.

Bartoszewicz, Mateusz. "Chiński System Zaufania Społecznego." *Przegląd Geopolityczny* 32, 2020: 58–67.

Cristianini, Nello, and Teresa Scantamburlo. "On Social Machines for Algorithmic Regulation." *AI & Society: Knowledge, Culture and Communication* 35, 2020: 645–62.

Kindt, Els J., and Catherine Jasserand. "Commentary on Article 5. Prohibited AI Practices." In *The EU Artificial Intelligence (AI) Act: A Commentary*, edited by Ceyhun Necati Pehlivan, Nikolaus Forgó, Peggy Valcke. Wolters Kluwer, 2024.

Raz, Aviad, and Jusaku Minari. "AI-Driven Risk Scores: Should Social Scoring and Polygenic Scores Based on Ethnicity Be Equally Prohibited?" *Frontiers in Genetics* 14, 2023: 1169580. https://doi.org/10.3389/fgene.2023.1169580.

Zhang, Mi. "Analiza Systemu Oceny Wiarygodności Społecznej z wykorzystaniem teorii Nudge." Master's thesis, Szkoła Główna Handlowa w Warszawie, 2021.

ZESZYT PRAWNICZY UAM
NR 15/2025
https://doi.org/10.14746/zpuam.2025.15.2

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

MIKOŁAJ JĘDRZEJCZAK

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0004-9764-0916
mikjed5@st.amu.edu.pl

Leading a Minor Under the Age of 15 to Engage in Any Other Sexual Activity in Cyberspace

Abstract: The article aims to define, through formal and dogmatic analysis, the scope of Article 200 § 1 of the Polish Criminal Code, which penalizes leading a minor under 15 to other sexual activity in the context of cyberspace. It emphasizes that committing this crime does not require physical presence and that cyberspace poses challenges in interpreting legal norms expressed through phrases and terminology typical of physical interaction. The article also addresses the victim's volitional and intellectual aspects. The conclusion presents a broad understanding of "leads to any other sexual activity", finding its application to the cyberspace. The subject of the article should be considered important in connection with the dynamic development of new technologies and increased Internet activity of minors.

Keywords: sexual freedom, cyberspace, criminal protection of a minor, limits of criminal liability

Introduction

Contemporary regulations included in the Polish Penal Code[1] provides protection for minors in the field of sexual freedom, reflection if which is Art. 200 § 1 of the p.c., which criminalizes the sexual abuse of a minor under the age of 15. The elements of this crime are fulfilled by a person who has sexual intercourse with a minor under the age of 15 or commits any other sexual act against such a person or leads them to undergo or perform such activities.[2] The cited provision, through the scope of the aforementioned elements of commission acts, is applicable in a wide range of factual situations. Moreover, the application of this provision takes on particular importance in connection with the dynamic development of new digital technologies and increased Internet activity of minors, who are particularly vulnerable to sexual abuse by offender. The combination of a wide spectrum of behaviours penalized by the norm with the prevalence of paedophilic behaviour in the digital space encounters interpretation problems in the scope of the objective and subjective side of the prohibited act. Although some of the above-mentioned elements of commission activities (i.e. "sexual intercourse" or "any other sexual activity") refer *stricte* to hand-held behaviour, the designation of which is physical contact in the real world, so the element "leads" does not determine the need for the offender to

[1] Ustawa z dnia 6 czerwca 1997 r.—Kodeks karny (consolidated text Journal of Laws of 2025, item 383), hereinafter: p.c.

[2] Lech Gardocki, *Prawo karne* (Wydawnictwo C.H. Beck, 2023), 287.

participate in the behaviour undertaken by the minor.[3] It is therefore a matter of penalizing a situation in which a minor under the age of 15 is involved in a sexual activity that does not involve physical contact with the person or persons committing that activity.[4]

The research objective of this article is to define, through the formal and dogmatic analysis, the scope of application of the legal norm contained in Art. 200 § 1 of the Criminal Code, focused on the interpretation of the element of commission act "leads to … any other sexual activity" in the context of committing such actions in the digital space to a minor under the age of 15. The problem of the offender's contact with the victim and offender's existence or non-existence in the material world will be analysed in relation to the implementation of conditions fulfilling the elements of a commission act through information system, including the characteristics of cyberspace as a place of leading to any other sexual activity with a minor and its impact on the volitional and intellectual aspect of a minor under the age of 15 in the context of the aforementioned crime.

Therefore, the considerations will concern only one of several commission acts that violate the sexual freedom of the minor, provided for by the legislator. The scope of the research will focus only on the form of offender, not including the offense of electronic sexual corruption of a minor related to the crime in question, regulated in Art. 200a of the p.c., which constitutes a *sui generis* offense of attempting to sexually abuse a minor. Narrowing the research field will allow the existence or non-existence of a construction gap in relation to paedophilic behaviour to be demonstrated. This problem is particularly important in connection with the dynamic development of new digital technologies and increased Internet activity of minors, who are particularly vulnerable to sexual abuse by offender.

1. Leading to Any Other Sexual Activity as an Act of Committing a Prohibited Act in the Context of Cyberspace

The history of crimes against sexual freedom and the relatively short period of popularity of online communicators enabling audiovisual contact raise doubts as to the possibility of leading a minor to another sexual activity in cyberspace. It is clear in relation to the cited feature of commission action that it is possible to lead a minor under the age of 15 to sexual intercourse or to undergo another sexual ac-

[3] Jarosław Warylewski and Katarzyna Nazar, "Commentary on Article 200," in *Kodeks karny: Komentarz*, ed. Ryszard Andrzej Stefański (Wydawnictwo C.H. Beck, 2023), 1404.

[4] Marek Bielski, "Commentary on Article 200," in *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117–211a*, ed. Włodzimierz Wróbel and Andrzej Zoll (LEX/el., 2018).

tivity or to perform such an activity by violence, threat or deception, and it is even sufficient to use low-intensity forms of violence.[5] However, it should be determined whether the induction of any other sexual activity is carried out not only without physical coercion on the part of the offender, but also whether it can take place only through social communicators (which are a form of information system), without prior psychophysical contact outside cyberspace.

"Any other sexual activity" may consist not only of the physical but also of the intellectual involvement of the victim, when it is objectively sexual in nature, which, however, does not fall within the concept of "sexual intercourse".[6] It occurs, for example, when the offender leads the victim to observe the masturbating person.[7] Despite the fact that the term in question does not have a legal definition, the scope of its application is wide enough to apply to a number of behaviours characterized by passive participation in a given sexual activity, or even the exclusive performance of such an activity by him, without the participation of the offender. Of course, it is possible to lead to a sexual act using physical coercion (for example, committing this offence in connection with bringing a minor to a sexual act with a third party, using physical force to perform sexual contact), but the phrase "any other sexual activity" is not an accessory to the physical contact of the offender with the victim. This, such an activity can also find its application by exploiting the inability to properly understand reality by a minor, by blackmail or threat manifested only in speech. However, it is not required that the offender performs a physical act. Moreover, this does not apply to the presence of the offender, which would condition the commission of the crime.

Leading to any other sexual activity is used in isolation from material reality also due to the above-mentioned phrase "leads", which with its universal meaning also goes beyond the traditional, physical framework of the offender's behaviour towards the victim. Use in Art. 200 § 1 of the p.c. of this word opens the way to the recognition that the offender of this act may be a person acting via the Internet—leading the minor via the Internet to the behaviours indicated in Art. 200 § 1 of the p.c.[8] The key aspect, apart from the lack of the need for the offender's personal action in committing such an action, is the recognition of current social messengers as a space that can be qualified as a place for committing a crime. It must condition the existence of a causal relationship between the offender's committing a specific behaviour (which is not material contact) and the occurrence of an act with a minor

[5] Błażej Kolasiński and Dorota Korecka, "Przestępstwa pedofilskie w Kodeksie karnym," *Prokurator* 18, no. 2 (2004): 31.

[6] Jarosław Warylewski, "Glosa do uchwały SN z dnia 19 maja 1999 r., I KZP 17/99," *Orzecznictwo Sądów Polskich*, no. 12 (1999): 224.

[7] Warylewski, "Glosa do uchwały SN z dnia 19 maja 1999 r., I KZP 17/99," 224.

[8] Barbara Kunicka-Michalska, "Pornografia i wykorzystywanie nieletnich w Internecie: Regulacje polskiego kodeksu karnego," *Studia Prawnicze* 166, no. 4 (2005): 77, https://doi.org/10.37232/sp.2005.4.4.

under the age of 15, which can be considered a sexual act. It should be noted that leading to any other sexual activity, unlike other cases conditioned by commission activities under Art. 201 § 1 of the p.c., is a material crime. In the analysed case, the effect required by law is to lead a minor under the age of 15 by the offender to undergo a sexual act.[9] The basis for criminal liability may be the undertaking of behaviour that should be objectively considered as the reason for a minor under 15 years of age to undergo a given type of sexual activity.[10]

Modern technologies make it possible not only to send text messages, the content of which may encourage minors to perform sexual activities (e.g. masturbation), but also to transmit sound and image by sending videos or conducting live broadcasts. The use of such measures thus makes it possible to present pornographic content or distribute it in a way that allows the minor to become acquainted with it.[11] Therefore, in view of the cited facts, it should be stated that if a social communicator (being a form of an information system) is able to be a place constituting a designate for the presentation of paedophilic content, it is also a place allowing for the delivery of a statement the content of which leads the minor to perform any other sexual activity, which in turn is a designate of the behaviour penalized by the analysed norm. This usually involves the recording and delivery via an audiovisual system or network of another sexual activity that the offender is familiar with. However, it is reasonable to specify that such a recording does not necessarily always need to be sent. After all, executive action has been described in this case as any form of physical or mental influence leading to sexual activity involving a minor under the age of 15.[12] However, such a case is far from reality, because in the situation of its occurrence the offender would not be entitled to emotional satisfaction related to the criminological background and purposefulness of the crime in question. Nevertheless, it should be stated that the very action in the online sphere culminates in another sexual activity involving a minor, without the offender becoming acquainted with it in the sensual aspect, would be applicable to this norm. However, this involves significant procedural difficulties in evidence, which are not the subject of the discussion undertaken here.

Therefore, it should be assumed that due to the linguistic interpretation contained in the legal norm of phrases, it is clearly possible to commit the offence of bringing a minor under the age of 15 to any other sexual activity in cyberspace. This is not only due to the lack of any need for the physical aspect of the offender in relation to the victim of this element, but also due to the nature of the social messenger, which is a place allowing for such sexual activity to be implemented in

[9] Warylewski and Nazar, "Commentary on Article 200."

[10] Bielski, "Commentary on Article 200."

[11] Maciej Siwicki, "Ochrona małoletniego przed konfrontacją z treściami pornograficznymi," *Państwo i Prawo* 790, no. 12 (2011): 76.

[12] Bielski, "Commentary on Article 200."

cyberspace. Behaviour is the only case of direct use of a minor, of those behaviours contained in Art. 200 § 1 of the p.c., which is possible to implement in cyberspace as a place of crime. This conclusion is particularly important because it establishes the possibility of subsuming a significant number of facts whose place of commission of the crime is cyberspace to Art. 200 § 1 of the p.c., and clarifying the norm contained therein. This is associated with a more severe criminal penalty than in the case of presenting content of a paedophilic nature to a minor or a wide range of activities aimed at committing the crime in question, which was established in Art. 200a of the p.c., where the information system or network plays a special role.

The application of such a broad scope of the impact of criminal law protection should be deemed justified. Paedophilic behaviour is increasingly taking place in cyberspace, which is related to the obvious spread of new technologies in everyday life, including the life of minors under the age of 15. Taking into account the axiological basis of the functioning of the norm and the damage to the mental development of the victim led to any other sexual activity that may affect future mental conditions, no change in the interpretation of the article's wording should be postulated. By their linguistic meaning, even in their colloquial use, phrases clearly emphasize the diverse behaviours that can be classified to them. Therefore, it should be concluded that applying them also to cyberspace does not violate the principle of *nullum crimen sine lege certa*.

2. The Importance of Cyberspace as a Place of Crime

It is justified to consider how cyberspace as a place of committing a crime affects the occurrence and definition of some objective elements of a prohibited act, in the context of the element "leads to any other sexual act" and what its characteristics are. However, it should be clearly stated that where cyberspace is the place of committing the crime of leading to any other sexual activity with a minor under 15 years of age it is difficult, though not impossible, to find objective elements of the crime.

Problems start with the very attempt to properly apply the phrase "cyberspace" in terms of definition. This phrase has a legal definition, although this is not the same as other similar phrases, such as "digital space" or the Internet. The legal literature lacks a uniform interpretation, the result of which would be the commonly used *definiens* of these two other phrases, especially "digital space". This undoubtedly results from the requirements that are associated with such a challenge, not only in the field of knowledge about the law, but also in the field of technical knowledge about new technologies.

In relation to the analysed phenomenon, the most relevant would be the use of the concept of "cyberspace". Despite its most common occurrence in relation to the threat to the state's IT security, this expression is associated with phrases more

firmly established in the law by having a legal definition. It is also often invoked in the context of prohibited acts. Cyberspace under Polish law is understood as a space for processing and exchange of information created by information systems, referred to in Art. 3 point 17 of the Act of 17 February 2005 on computerization of the activities of entities performing public tasks,[13] along with links between them and relations with users.[14] An informatic system is a set of IT equipment and software, providing processing and storage, as well as the functionality to send and receive data through telecommunications networks using a terminal device appropriate for the type of network, commonly called the Internet.[15] This suggests that such a system concerns a wider scope than a telecommunications network, which does not have to be based on an Internet connection, as exemplified by a telephone call or sending SMS messages. These methods of communication are based on a narrower range of technical solutions. The doctrine presents sentences specifying the area using the phrase "cyberspace". This is a kind of communication space created by the system of Internet connections.[16] Cyberspace equally includes the Internet, telecommunications networks or computer systems, and therefore all IT systems included in the global network.[17] The connection with the global aspect is connected with a separate issue of determining the place in which a crime is committed in connection with such systems.

An analysis of the very legitimacy of the use of the phrase "cyberspace" encounters a multiplicity of related specialist phrases, but it outlines the framework for the further part of discussion regarding bringing a minor under the age of 15 to any other sexual activity. Due to the fact that this phenomenon constitutes a material crime, there must also be a result, as already established earlier. The lack of objective predictability of a criminal result in a given factual situation excludes the possibility of behaving in accordance with the rules of conduct, and therefore excludes the recognition of such behaviour as an object to the application of the norm.[18] Moreover, the result as a state separated from the behaviour of the offender should lie "outside" this behaviour.[19] In the absence of a tangible change in the external world included in the type of prohibited act, the result will also not indicate the direction

[13] Consolidated text Journal of Laws of 2024, item 1557 as amended.

[14] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (consolidated text Journal of Laws of 2025, item 504).

[15] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (consolidated text Journal of Laws of 2024, item 1513).

[16] Katarzyna Chałubińska-Jentkiewicz, "Cyberbezpieczeństwo—zagadnienia definicyjne," *Cybersecurity and Law* 2, no. 2 (2019): 6, https://doi.org/10.35467/cal/133828.

[17] Cezary Banasiński, "Pojęcie cyberprzestrzeni," in *Cyberbezpieczeństwo: Zarys wykładu*, ed. Cezary Banasiński (Wolters Kulwer, 2023), 23–27.

[18] Judgment of the Supreme Court of the Republic of Poland of October 12, 2016, V KK 153/16, LEX no. 2151447.

[19] Elżbieta Hryniewicz, "Skutek w prawie karnym," *Prokuratura i Prawo*, no. 7–8 (2013): 118.

of the offender's behaviour in the type of prohibited act.[20] It is crucial to find a rationalization for recognizing cyberspace as a place where the offender's behaviour or a perceived change in the external world takes place in order to determine the elements of the objective matter, which is a structural element of this prohibited act.

A prohibited act is deemed to have occurred at the place where the offender acts or fails to perform an action that the offender is obliged to perform, or where the results of the prohibited act take place, or are intended by the offender to take place. The activity of the offender in cyberspace is not controversial, as activities that are related to bringing a minor to any other sexual activity and are noticeable in the communication space constituting it are behaviours that allow the offender to be blamed for a prohibited act. Therefore, activities using devices connected to the communication space (including the formulation of threats or suggestive statements) allow for their recognition as activities in the digital space, which implies this can be classified as the place of the crime. It is more difficult to determine the existence of a result. The material environment of a minor performing another sexual activity can be clearly defined as the place of the result: it will always be the place where the crime is committed. However, it seems more ambiguous to recognise cyberspace as the place of the result. This is due to the fact that there may be a situation in which the minor does not prepare an audiovisual form, such as a photo or recording. As a result, the action will not leave any trace in cyberspace. Therefore, one would be inclined to reflect that cyberspace will be the place where the results takes place, but only if there is a trace in the information system of the minor person subjected to such sexual activity. In the strict sense of the word, we call a perceptible system of things or a phenomenon caused by someone due to the fact that some form of expression established or customarily shaped rules dictate that thoughts of a specific type must be associated with this system.[21] The signs in this case will be any activities that can be considered objectively sexual, which have been recorded on a data carrier in an information system that can be sensually recognized (usually visual).

The heterogeneity and complexity of cyberspace as a place where a crime is committed renders it difficult to deconstruct some objective elements of a prohibited act. However, it is possible, following a logical and linguistic analysis, to consider this phenomenon as the place where the crime was committed. This is due to the possibility of taking action in it by the offender of the prohibited act and the conditional occurrence of the result of leading to another sexual act in it. It is also important to emphasize the nature of technical devices or messages sent through them as tools for committing a crime. This allows for a more complete deconstruction of the crime and the separation of cyberspace as a broader phenomenon with elements constituting it as a place, not a tool. Recognising cyberspace as a place

[20] Hryniewicz, "Skutek w prawie karnym," 118.

[21] Zygmunt Ziembiński, *Logika praktyczna* (Wydawnictwo Naukowe PWN, 2014), 14.

of crime should be considered justified. Due to the increasing role of information technology in interactions between offenders and victims of crimes against sexual freedom, elements related to cyberspace must be integral to the site of the crime. However, the same extent is associated with the considerable diversity of phenomena on technical grounds, which, due to having different characteristics and scopes of application, lack legal definitions. This makes it difficult to properly apply the law on the basis of diverse facts related to modern technologies. Therefore, it should be postulated to create definitions that are legal under national law, such as "digital space" or "Internet", because the jurisprudence applies these phrases instrumentally *in concreto*, without outlining a universal *definiens*.

3. The Impact of Cyberspace on the Volitional and Intellectual Aspect of the Victim

An offence under paragraph 200 § 1 of the p.c. may be committed only intentionally, whereas it is generally assumed that the form of intention may be direct intention or quasi-eventual intention.[22] In the case of the volitional and intellectual aspect of the offender, cyberspace does not play a significant role, because the said intention is born in him, even before his contact with cyberspace, and is made visible by the actions taken during the attempt to commit the act. In the case of a proposal regarding sexual intercourse, submission to or performance of any other sexual act, the actions taken by the offender in the phase of aiming to implement the proposal should differ from the mere contact with the victim as part of the process of submitting a sexual proposal to them, and clearly bring the offender closer to its implementation in analogue reality.[23] Intellectual abilities and the volitional aspect are also relevant in the context of the victim. The element "leads" assumes the existence of a causal relationship between the offender's act and the undertaking of specific behaviours by a minor, but it is important that the offender in this system is the active party, and without his initiative, the act would not have taken place.[24] To clarify, the legislator in Art. 200 § 1 of the p.c. using the concept of "leads" to the exclusion of activities in which the offender does not himself lead the minor to sexual activity, and participates in it as a result of the minor's behaviour.[25] This raises the question of whether, and if so, how cyberspace affects the volitional and intellectual aspect of a minor under the age of 15 in the context of the prohibited act

[22] Warylewski and Nazar, "Commentary on Article 200."

[23] Mikołaj Małecki, "Fazy groomingu: Glosa do postanowienia SN z dnia 17 marca 2016 r., IV KK 380/15," *Przegląd Sądowy* 27, no. 1 (2018): 112–13.

[24] Kolasiński and Korecka, "Przestępstwa pedofilskie w Kodeksie karnym," 31.

[25] Judgement of the Supreme Court of the Republic of Poland of May 16, 2008, I KK 338/07, LEX no. 435275.

under analysis. Special clarification is required in the case of a minor performing any other sexual activity, without external pressure or maturity, which could be classified as *vis compulsiva*.

A minor performing any other sexual activity in cyberspace does not have to experience external coercion to perform it. It is true that cyberspace is a place where blackmail or the threat can occur, which obviously violates the free will of the victim. However, the prohibited act might only be carried out through suggestive statements that would encourage, but not force, sexual activities such as touching in intimate places or masturbation. However, the standard will not apply at all if the minor fully independently takes the aforementioned initiative to perform such an activity. However, this will only happen if the minor's will is not violated by any actions of the offender, even allowing the minor to take such an initiative in cyberspace or in the physical world. Because the offender who actively proposes tangible benefits in exchange for certain conduct, provides transport, makes the premises available, facilitates playing on the computer, or shows activity aimed at obtaining the intended and should be added non-contradictory result with the will of minors in the form of either sexual intercourse or undergoing any other sexual activity, thereby realizes the element of "leads".[26] All these situations, which modify or do not affect the will of the minor, can take place both in cyberspace and in the material world. This leads to the reflection that cyberspace does not have any extraordinary impact on the volitional aspect of the victim.

A precisely different situation takes place in the context of cognitive abilities, related to the intellectual aspect, in the case of a victim of such a crime. Cyberspace may impact the awareness of the minor as to the form of the offender. Using online platforms or communicators operating in the ICT system, the offender has the opportunity to create a false identity. This may take the form of aspects such as communicating with a minor in cyberspace, impersonating a person close in age to the victim, or creating in them a belief that a paedophile situation does not exist. In the present case, even with the implementation of an exclusive initiative on the part of a minor, there is no situation excluding the application of the norm, by creating a false image of reality through deception, which should be treated not only as an active action that aimed at committing a crime, but also the exploitation of the victim's inability to properly perceive reality, which is based on ongoing intellectual development. This will be of particular importance where there is a small age difference, which would prejudge the existence of a crime, an example of which would be the commission of such a prohibited act by a minor who was only 17 years of age.

The conclusions lead to an unambiguous reflection that despite the lack of any impact of cyberspace on the volitional aspect of minors in the offence of leading to any other sexual activity, it is important for their cognitive functions and awareness

[26] Judgement of the Supreme Court of the Republic of Poland of May 16, 2008, I KK 338/07.

of the implementation of the prohibited act by the offender. Modern technologies, by misleading, can easily lead to interference in the intellectual sphere of a minor under the age of 15.

Summary

The linguistic interpretation contained in the legal standard under Art. 200 § 1 of the p.c. of the phrases "punishing", or "bringing a minor under the age of 15 to any other sexual activity" clearly indicates the possibility of committing a crime in cyberspace. This is due not only to the lack of a need for the offender's physicality in relation to the victim, but also to the communicator, which is a form of an information system that can be treated as an element allowing for their implementation. The heterogeneity and complexity of cyberspace as a place where a crime is committed makes it difficult to deconstruct some objective elements of the prohibited act. However, it is possible, following a logical and linguistic analysis, to consider this as the place where the crime was committed. This is due to the possibility of taking action in cyberspace by the offender of the prohibited act and the conditional occurrence of the result of leading to any other sexual act in it. The diversity and high technical knowledge needed to properly classify new technologies makes it reasonable to consider creating new legal definitions outlining the semantic framework of phrases related to these technologies, allowing for their potentially more effective use in order to effect more precise and effective protection of goods by criminal law standards. Cyberspace itself may constitute an element affecting the intellectual sphere of a minor who, by not believing that a situation might involve a paedophile element, may demonstrate an initiative to perform an act of a sexual nature. This illustrates the complexity of the problem of bringing a minor under the age of 15 to any other sexual activity in cyberspace. Undoubtedly, although it does not make it impossible, it has a significant impact on the effectiveness of deconstructing the objective elements of the crime and on the minor himself in the analysed case, blurring the clear boundaries of criminal liability.

BIBLIOGRAPHY

Banasiński, Cezary. "Pojęcie cyberprzestrzeni." In *Cyberbezpieczeństwo: Zarys wykładu*, edited by Cezary Banasiński. Wolters Kulwer, 2023.

Bielski, Marek. "Commentary on Article 200." In *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117–211a*, edited by Włodzimierz Wróbel and Andrzej Zoll. LEX/el., 2018.

Chałubińska-Jentkiewicz, Katarzyna. "Cyberbezpieczeństwo—zagadnienia definicyjne." *Cybersecurity and Law* 2, no. 2(2019): 7–23. https://doi.org/10.35467/cal/133828.

Gardocki, Lech. *Prawo karne*. Wydawnictwo C.H. Beck, 2023.

Hryniewicz, Elżbieta. "Skutek w prawie karnym." *Prokuratura i Prawo*, no. 7–8 (2013): 106–26.
Kolasiński, Błażej, and Dorota Korecka. "Przestępstwa pedofilskie w Kodeksie karnym." *Prokurator* 18, no. 2 (2004): 22–43.
Kunicka-Michalska, Barbara. "Pornografia i wykorzystywanie nieletnich w Internecie: Regulacje polskiego kodeksu karnego." *Studia Prawnicze* 166, no. 4 (2005): 77–108. https://doi.org/10.37232/sp.2005.4.4.
Małecki, Mikołaj. "Fazy groomingu: Glosa do postanowienia SN z dnia 17 marca 2016 r., IV KK 380/15." *Przegląd Sądowy* 27, no. 1 (2018): 107–15.
Siwicki, Maciej. "Ochrona małoletniego przed konfrontacją z treściami pornograficznymi." *Państwo i Prawo* 790, no. 12 (2011): 68–79.
Warylewski, Jarosław. "Glosa do uchwały SN z dnia 19 maja 1999 r., I KZP 17/99." *Orzecznictwo Sądów Polskich*, no. 12 (1999): 224.
Warylewski, Jarosław, and Katarzyna Nazar. "Commentary on Article 200." In K*odeks karny: Komentarz*, edited by Ryszard Andrzej Stefański. Wydawnictwo C.H. Beck, 2023.
Ziembiński, Zygmunt. *Logika praktyczna*. Wydawnictwo Naukowe PWN, 2014.

ZESZYT PRAWNICZY UAM
NR 15/2025
https://doi.org/10.14746/zpuam.2025.15.3

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

MICHALINA KOZIŃSKA

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0009-1797-6054
mickoz9@st.amu.edu.pl

KAROLINA NALEWAJ

Nicolaus Copernicus University in Toruń, Poland
https://orcid.org/0009-0004-2905-6697
nalewaj@doktorant.umk.pl

Justification of Decisions According to Polish and European Standards

Abstract: The article analyzes the obligation to justify administrative decisions in the context of European legal standards and their implementation in Poland. The justification is presented as a foundation of the rule of law, ensuring transparency, accountability and protection of individual rights. Reference is made to Recommendation CM/Rec(2007)7, the European Code of Good Administrative Practice, jurisprudence and ReNEUAL principles. The Polish legal system, especially the Code of Administrative Procedure and Administrative Court Procedures, aligns itself with these norms. The article emphasizes the importance of justification for trust in administration and points out exceptions, such as in security cases. It also discusses the role of EU law and the challenges of technology, artificial intelligence systems and data protection.

Keywords: standards for justifying decisions, European Union law, European standards for administrative law, international law, good administration

Introduction

The justification of decisions and judgments is an essential element of the legal system and is key to upholding the rule of law and ensuring transparency, justice and the protection of individual rights. In the European context, various acts and legal instruments emphasize and regulate the importance of justifying decisions. The legal system is a complex structure comprising legal norms and institutions that regulate social behaviour and relations between individuals. It uses legal instrumentalization, that is, the right to create and implement strategies to achieve certain goals.[1] It is based on established norms and guidelines established by judicial authorities, which are often referred to as legal standards.[2] There will also be arguments that these standards are necessary to guarantee protection of the rights of individuals and to ensure fairness regarding any decisions made by public authorities. Given the importance of legal standards, this article also aims to raise awareness and boost understanding of their role in the current legal order. In lexicographic studies, the

[1] Sławomira Wronkowska, "Kilka tez o instrumentalizacji prawa i ochronie przed nią," *Przegląd Prawa i Administracji* 110, no. 3 (2017): 107–10, https://doi.org/10.19195/0137-1134.110.8.

[2] Wronkowska, "Kilka tez o instrumentalizacji prawa i ochronie przed nią," 107–10.

word "standard" is identified with the average standard, type, pattern, model, also with the product corresponding to established characteristics regarding its quality, weight, measure and composition.[3]

1. The Standard of Justification in Decision-Making Under European Legal Norms

In order to fully understand how the obligation to justify decisions functions within the European legal framework, it is necessary to examine both the concept of legal standards and their normative sources. This analysis requires consideration of the theoretical foundations, international regulations, and the practical implications for national legal systems. The following section explores the nature of legal standards and the role they play in shaping administrative and judicial decision-making processes.

The justification of decisions and judgments is an essential element of the legal system and is key to upholding the rule of law and ensuring transparency, justice and the protection of individual rights. In the European context, various acts and legal instruments emphasize and regulate the importance of justifying decisions. The legal system is a complex structure comprising legal norms and institutions that regulate social behaviour and relations between individuals. It uses legal instrumentalization, that is, the right to create and implement strategies to achieve certain goals.[4] It is based on established norms and guidelines established by judicial authorities, which are often referred to as legal standards.[5] There will also be arguments that these standards are necessary to guarantee the protection of the rights of individuals and to ensure fairness regarding any decisions made by public authorities. Given the importance of legal standards, this article also aims to raise awareness and boost understanding of their role in the current legal order. In lexicographic studies, the word "standard" is identified with the average standard, type, pattern, model, also with the product corresponding to established characteristics regarding its quality, weight, measure and composition.[6]

The thesis of this article is that the Polish legislator meets the European standard for introducing an obligation to justify decisions. In addition, it will show why they are necessary in the current legal system. The requirements for justifying decisions that are imposed by European legal standards will be analysed in detail, and why they should be observed by adjudicating bodies and public institutions.

---

[3] Małgorzata Jaśkowska, *Standardy współczesnej administracji i prawa administracyjnego* (Wolters Kluwer Polska, 2019), 9.

[4] Wronkowska, "Kilka tez o instrumentalizacji prawa i ochronie przed nią," 107–10.

[5] Wronkowska, "Kilka tez o instrumentalizacji prawa i ochronie przed nią," 107–10.

[6] Jaśkowska, *Standardy współczesnej administracji i prawa administracyjnego*, 9.

The publication also aims to show that these standards help maintain transparency and fairness in decision-making, which is crucial for the rule of law, since the rule of law is not just about creating new regulations or sanctions, but also about adhering to certain standards that ensure that the processes are transparent, predictable and equitable.[7]

In this context, the standard can be described as a benchmark that serves to regulate the practice of law in general and is placed between a specific ruling and an abstractly existing provision.[8] The standard, which stems from international law and relates to the obligation to shape procedure in decision-making, is the need to provide reasons for decisions. The procedural fairness standard covers all stages of national legal procedures that apply to a particular case.[9]

It is also important to approach the issue of an administrative decision as a unilateral act issued by an authority based on applicable law. This is because it resolves issues concerning the rights and obligations of citizens, which involve the responsibility of the public administration body that issues it. For this, the decision itself is an individual, authoritative and unilateral administrative act. In the context of certain European and international acts, the concept of decision may have a broader meaning, including acts of a general nature.[10]

The principle of justifying decisions is a fundamental element of fair and equitable proceedings under international law. Among other things, it imposes an obligation on international bodies and institutions and states. The justification of decisions helps to ensure transparency, fairness and control in decision-making processes, and thus enables parties or interested parties to receive a clear, consistent and detailed explanation of why a decision was made. The criterion for assessing the national standard of legal protection is the European convention (Strasbourg) or treaty (Luxembourg) standard. Poland, being a member of the Council of Europe and the European Union (EU), is obliged to respect these standards. Belonging to the European legal culture obliges the national legislator to respect the standards and concepts of human rights protection, established by the international community; moreover, the standards related to administrative proceedings—especially in the field of justification of decisions—should be considered today as a component of the set of human rights.[11]

Meanwhile, in the context of new technologies, artificial intelligence and the protection of personal data, European standards for justifying decisions take on

[7] Jeremy Waldron, "Positivism and Legality: Hart's Equivocal Response to Fuller," *NYU Law Review* 83, no. 4 (2008): 1137.

[8] Mariola Żak, "Pojęcie standardu prawnego w sieciowym systemie prawa," *Przegląd Prawa Publicznego*, no. 1 (2019): 8.

[9] Żak, "Pojęcie standardu prawnego w sieciowym systemie prawa," 8.

[10] "Decyzja administracyjna—odwołanie, skarga," Wolters Kluwer, https://www.wolterskluwer.com/pl-pl/solutions/lex/administracja/prawo/decyzja-administracyjna, accessed 23 November 2024.

[11] Żak, "Pojęcie standardu prawnego w sieciowym systemie prawa," 17.

particular importance. Technological developments, including the automation of decision-making processes, require clear and transparent justification of administrative and judicial decisions to ensure the transparency of artificial intelligence-based systems and the protection of individual rights. The obligation to justify decisions around data protection is crucial to ensure compliance with the General Data Protection Regulation, which requires decisions based on profiling or algorithms to be understandable and capable of being challenged. Thus, European standards in this area supply the framework not only for the rule of law, but also for the ethical and responsible use of new technologies in the legal system.

2. Sources of Standards Related to the Conduct of Administrative Proceedings

The sources of law that establish standards related to the conduct of administrative proceedings derive from international law and domestic law, among other sources. They are examined by analysing the concept of the right to good administration, which is an important element of European administrative law. This aspect of the law underscores the existence of several different principles, covering material, organizational and procedural aspects. It is worth noting that the current Recommendation CM/Rec(2007)7 of the Committee of Ministers of the Council of Europe is devoted entirely to "good administration."[12] In this recommendation, we find many already-known principles, but also new regulations.[13] From our perspective, the right to good administration is important, which will be addressed later in the article.

In the context of this recommendation, one of the most important aspects is the requirement to justify each individual administrative decision. This standard applies broadly to the justification of actions taken by the administration, which is based on the belief that the administration acts deliberately. According to the provisions of the Code of Administrative Procedure, every individual administrative decision must be justified, at least in matters that affect the rights of individuals. It is worth emphasizing that this justification is significant because it allows understanding the basis of the decisions made.[14]

The basic principle expressed in Recommendation CM/Rec(2007)7 is the rule of law, which dictates that public administration bodies act in accordance with

[12] Recommendation CM/Rec(2007)7 of the Committee of Ministers to member states on good administration, adopted by the Committee of Ministers on 20 June 2007 (consolidated text Council of Europe: Committee of Ministers), hereinafter: Recommendation CM/Rec(2007)7.

[13] Grzegorz Krawiec, "Europejskie standardy związane z przebiegiem postępowania administracyjnego," *Roczniki Administracji i Prawa*, no. 1 (2011): 70.

[14] Marcin Princ, *Standardy dobrej administracji w prawie administracyjnym* (Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza, 2016), 263.

the law.[15] This means that the administration cannot take arbitrary action, even if acting within its discretion.[16] In this respect, the law includes both domestic and international laws, as well as general rules for organization, operation and activities.[17]

The CM/Rec(2007)7 Recommendation also includes the principle of equality, stating that individuals in the same situation should be treated with equal rights and principles.[18] No form of discrimination, whether based on gender, ethnicity, religion or other aspects, is acceptable.[19] Most importantly from our perspective, differences in treatment must be objectively justified.[20]

Another principle expressed in Recommendation CM/Rec(2007)7 is that of impartiality.[21] This principle states that it is required to act objectively, considering only those circumstances relevant to the consideration.[22]

The guidelines indicated are central elements of general principles that have long existed both in the jurisprudence of the courts and in documents such as the European Code of Good Administrative Practice[23] and other legislation. At the same time, these principles apply at every stage of the administrative process, including during investigation procedures.[24]

Justification of decisions is a legal standard in many European laws and venues, both nationally and internationally, as also evidenced by the European Court of Justice (ECJ). The ECJ's jurisprudence often emphasizes the importance of justifying decisions made by European institutions and national authorities in the context of European Union law. According to the ECJ, member states should have an effective judicial review of the legitimacy of decisions, as their justification is crucial in the context of human rights and providing protection to the individual from the arbitrariness of administrative bodies' decisions. Thus, it can be said that there are common standards valued at both the national and European levels, and adherence to these principles is the basis for the functioning of a democratic state under the rule of law.[25]

The European Convention on Human Rights (ECHR) is an international convention that was adopted by the Council of Europe in 1950, which is also a key

[15] Art. 2 para. 1, Recommendation CM/Rec(2007)7.

[16] Art. 2 para. 1, Recommendation CM/Rec(2007)7.

[17] Art. 2 para. 2, Recommendation CM/Rec(2007)7.

[18] Art. 3 para. 1, Recommendation CM/Rec(2007)7.

[19] Art. 3 para. 2, Recommendation CM/Rec(2007)7.

[20] Krawiec, "Europejskie standardy związane z przebiegiem postępowania administracyjnego," 70.

[21] Art. 4, Recommendation CM/Rec(2007)7.

[22] Art. 4, para. 2, Recommendation CM/Rec(2007)7.

[23] European Ombudsman, The European Code of Good Administrative Behaviour (European Union, 2015), https://www.ombudsman.europa.eu/en/document/en/3510, accessed 23 November 2024, hereinafter: GAC.

[24] Krawiec, "Europejskie standardy związane z przebiegiem postępowania administracyjnego," 71.

[25] Court of Justice of the European Union (CJEU), press release no. 70/13, Luxembourg, 4 June 2013, Judgment in Case C-300/11 *ZZ v. Secretary of State for the Home Department*: The essence of the reasons for a decision refusing entry into a Member State must be disclosed to the person concerned, https://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130070en.pdf, accessed 11 November 2024.

element in shaping administrative procedure. The Convention, being the document that regulates the protection of human rights and fundamental freedoms in Europe, established the European Court of Human Rights (ECtHR), which was established under the Convention.[26]

The Convention imposes an obligation on signatories to bring their national laws and practices into line with the norms and standards set forth in the ECHR. In practice, this means that member states must ensure the protection of rights and freedoms such as the right to life, freedom from torture, freedom of expression, freedom of religion, the right to a fair trial and many others.[27] The ECtHR, which operates under the ECHR, is authorized to hear complaints from individuals or organizations that believe their rights under the Convention have been violated by a member state. The Court can issue judgments in such cases and recommend compensation to aggrieved parties.[28]

In this way, the ECHR plays an important role in shaping procedures and standards for the protection of human rights in Europe, and in the enforcement of these rights at the international level. Member States of the Council of Europe have pledged to abide by the Convention and its rulings, which is an important part of the European system of human rights protection.[29]

A particularly relevant document is the Code of Good Administration, established by the European Parliament on 6 September 2001. The Code applies to the officials of EU institutions, but the literature points out that it can also be regarded as a set of standards useful outside the EU for assessing the performance of the administration.[30] Therefore, there is no contraindication to finding these standards useful in defining the duties of the "Polish" administration. This has the effect of bringing administrative law, including even the daily interactions of the citizen with administrative bodies, into line with the requirements of the EU. The principles contained in this Code have both substantive and procedural aspects.[31]

The model rules of administrative procedure developed by academics and practitioners as part of the ReNEUAL European Union Administrative Law Research Network are also a significant source of law. The indicated model rules are intended to reinforce the general principles of European Union law and codify best practices identified in EU law and national legal orders.[32]

---

[26] European Court of Human Rights, European Convention on Human Rights, https://www.echr.coe.int/documents/d/echr/convention_eng, accessed 23 November 2024.

[27] Art. 1–3, 6, 9–10, ECHR.

[28] Chapter II, ECHR.

[29] Art. 59, ECHR.

[30] Krawiec, "Europejskie standardy związane z przebiegiem postępowania administracyjnego," 70.

[31] Krawiec, "Europejskie standardy związane z przebiegiem postępowania administracyjnego," 71.

[32] Paul Craig, "Introduction to the ReNEUAL Model Rules / Book I—General Provisions," in *ReNEUAL Model Rules on EU Administrative Procedure*, ed. Herwig C.H. Hofmann et al. (Research Network on EU Administrative Law, 2014), 3.

ReNEUAL's model regulations are not standards of administrative law in the sense of traditional legal acts. Rather, they are guidelines and models of conduct that can be used as models or inspiration for the creation of specific regulations and administrative acts. They do not contain a specific right to justify decisions but suggest principles that can be taken into account when issuing administrative decisions.[33]

In summary, ReNEUAL's model regulations are not standards identical to traditional administrative law, but are a tool for creating specific administrative regulations. They do not explicitly include the right to justify decisions but promote general principles and best practices in administrative proceedings in the European Union.[34]

The resolutions and recommendations of the Council of Europe, which will be discussed later in this article, should also be mentioned as a source of law. In the context of the principle of the right to good administration, contained in Article 41 of the Treaty on European Union, we can infer that the European Union attaches great importance to ensuring transparency, fairness and accountability in administrative processes. This right is fundamental to the democratic values that underpin the structure of the EU. They enable citizens living in the Union to participate in decisions that directly affect their lives.

Under Article 41, every citizen of the Union has the right to have his or her case heard impartially and fairly by the Union's institutions, bodies and agencies within a reasonable time. This right includes several key aspects, such as[35]:

1) The right to be heard: Every citizen has the right to be heard before individual measures are taken that may adversely affect him or her. This means that a person has the right to express his or her position and arguments on an issue before a decision is made;

2) The right to access his case file: every person has the right to access the documents and files of his case, but this right must be exercised with respect for the legitimate interests of confidentiality and professional and commercial confidentiality;

The duty of the administration to justify its decisions: the EU administration has an obligation to justify its decisions. This means that under EU law, the justification of decisions is as important as a party's active participation in the proceedings and access to documents—that is, justification has been placed among the foundations of good administration.[36]

All major European laws provide for the obligation to justify decisions, and consequently, it is placed very high in the hierarchy, which means that states should provide for such an obligation explicitly in their procedural laws.

---

[33] Craig, "Introduction to the ReNEUAL Model Rules," 3.

[34] Craig, "Introduction to the ReNEUAL Model Rules," 3.

[35] Charter of Fundamental Rights of the European Union (OJ C 326, 26.10.2012, pp. 391–407).

[36] Charter of Fundamental Rights of the European Union.

3. The Relevance of European Standards of Administrative Law for the Polish Legal System

The standards of European administrative law are fundamental to shaping the Polish legal system and ensuring the protection of citizens' rights and interests. In terms of Polish jurisprudence, the Supreme Administrative Court plays a key role in enforcing these standards. This is the highest judicial protection body within the structure of administrative courts in Poland, performing the function of adjudicating administrative cases, and ensures that the actions of the public administration are in accordance with the law and the principles of a democratic state under the rule of law. In exercising control over the actions of the administration, it is also concerned with the reasonable time for processing cases, compliance with the principle of fair procedure, but also with the effective protection of individual rights.[37]

When discussing the legislative process and the evolution of administrative law in Poland, it is worth mentioning European standards. Being a member of the Council of Europe, Poland is obliged to adapt its administrative law to international standards and the recommendations contained in the recommendations of the Committee of Ministers of the Council of Europe. This is an important part of Poland's integration into Europe and allows for consistency in laws and administrative procedures between member countries of the Council of Europe.[38]

In the already notorious case between the Republic of Poland and the EU on interim measures, the European Court of Justice unequivocally assessed that, in accordance with existing case-law, there is a principle of primacy, where it is the law of the Union that takes precedence over the law of the Member States.[39] This therefore presupposes that national authorities are obliged to meet the effectiveness of the Union's legal norms in their entirety, and the state cannot affect the effectiveness of these norms, within its territory.[40] As indicated, the fact that a national constitutional court rules in a particular way and invokes national laws in doing so cannot affect the CJEU's assessment because of the aforementioned principle of primacy.[41]

---

[37] Zbigniew Kmieciak, "Europejskie standardy prawa i postępowania administracyjnego a ustalenia orzecznictwa Naczelnego Sądu Administracyjnego," *Ruch Prawniczy, Ekonomiczny i Socjologiczny* 60, no. 1 (1998): 54.

[38] Kmieciak, "Europejskie standardy prawa i postępowania administracyjnego a ustalenia orzecznictwa Naczelnego Sądu Administracyjnego," 52.

[39] Order of the Court of Justice of October 27, 2021, C-204/21 R, LEX no. 3246811.

[40] Order of the Court of Justice of October 27, 2021, C-204/21 R.

[41] Order of the Court of Justice of October 27, 2021, C-204/21 R.

4. European Model of Decision Justification vs. Polish Model

The rationale for a decision in European law can be found in the aforementioned sources, which are Recommendation CM/Rec(2007)7, GAC, ECJ rulings, ReNEUAL model regulations or the Treaty on European Union.[42] According to him, each decision should be individual and include a justification that shows the expediency of the administration's action, at least in matters concerning the rights of individuals.[43] In addition, this is part of the fulfillment of the rule of law, which will directly show that public administration bodies take actions that are well thought out and provided for by law.[44]

It is also important to highlight the principles of good administration that affect the model for justifying decisions. Recommendation CM/Rec(2007)7 indicates the rule of law, the principle of equality, the principle of impartiality or the principle of proportionality. The Code of Good Administration consists of 27 articles, 24 of which relate directly to the organization of administration. There we can find such principles as the prohibition of abuse of power,[45] the principle of objectivity,[46] the principle of fairness[47] and the principle of courtesy,[48] the right to be heard and to make statements[49] and the obligation to justify decisions,[50] the principle of the rule of law,[51] the principle of non-discrimination,[52] the principle of proportionality[53] and the principle of impartiality and independence.[54] It also contains provisions on such aspects as the language of the letter,[55] the relevant time limits during the decision,[56] notification of the decision,[57] and the possibilities of appeal.[58]

---

[42] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 Tables of equivalences (OJ C 202, 7.6.2016, pp. 1–388).

[43] Princ, *Standardy dobrej administracji w prawie administracyjnym*, 263.

[44] Art. 2, para. 1, Recommendation CM/Rec(2007)7.

[45] Art. 7, GAC.

[46] Art. 9, GAC.

[47] Art. 11, GAC.

[48] Art. 12, GAC.

[49] Art. 16, GAC.

[50] Art. 18, GAC.

[51] Art. 4, GAC.

[52] Art. 5, GAC.

[53] Art. 6, GAC.

[54] Art. 8, GAC.

[55] According to Article 13 of the GAC, there is a rule to answer letters in the language of the citizen.

[56] Art. 17, GAC.

[57] Art. 20, GAC.

[58] Art. 19, GAC.

In the context of the ECJ's jurisprudence, it is worth noting the landmark judgment in Case C-222/86 *Heylens and Others*, in which the Court ruled that every administrative decision, especially one that affects the rights of an individual, must contain a statement of reasons that allows it to be understood and possibly challenged. The case concerned the recognition of professional qualifications, yet its significance goes beyond this specific matter, since it sets the standard for transparency and predictability of public administration action in the European Union. The judgment is also significant for Poland, as it indicates the obligation not only to justify decisions formally, but also substantively, in order to protect the rights of the individual and allow for an effective appeal. Similarly, the jurisprudence of the ECtHR emphasizes the importance of the right to a fair trial and openness of administrative proceedings, which is reflected in Article 6 of the ECHR.[59]

The Polish model of justifying decisions is clearly in alignment with European standards and recommendations contained in the recommendations of the Committee of Ministers of the Council of Europe.[60] We can find national regulations in the Code of Administrative Procedure or the Law[61] or the Law on Proceedings before Administrative Courts.[62]

The fact that the decision must contain a statement of reasons is also specified in the legislation.[63] It must include the facts considered by the authority as proven, an indication of the evidence considered in the case and the reasons for the evidence that was not taken into account and the legal basis on which it was based.[64] Polish jurisprudence emphasizes the fact that the decision and justification must be consistent,[65] and explain the reasoning of the authority and the reasons for the application of specific provisions.[66]

In shaping the standards of justifying administrative decisions in Poland, the case law of the Supreme Administrative Court and lower administrative courts plays a significant role. These courts have repeatedly emphasized that a decision's justification must not only be complete and logical but also allow the party involved to understand the legal and factual basis of the ruling. For example, in its judgment of 15 March 2012 (Case No. II GSK 59/11), the Supreme Administrative Court stated that the justification cannot simply refer to statutory provisions but must also ex-

[59] Judgment of the Court of Justice of October 15, 1987, 222/86, LEX no. 129587.

[60] Hereafter: CFR.

[61] Ustawa z dnia 14 czerwca 1960 r.—Kodeks postępowania administracyjnego (consolidated text Journal of Laws of 2024, item 572 as amended), hereinafter: KPA.

[62] Ustawa z dnia 30 sierpnia 2002 r.—Prawo o postępowaniu przed sądami administracyjnymi (consolidated text Journal of Laws of 2024, item 935 as amended), hereinafter: PPSA.

[63] Art. 107 § 1 Pt. 6, KPA.

[64] Art. 107 § 3, KPA.

[65] Judgment of the Provincial Administrative Court in Cracow of October 24, 2023, III SA/Kr 706/23, LEX no. 3622832.

[66] Judgment of the Provincial Administrative Court in Poznań of October 21, 2023, II SA/Po 368/22, LEX no. 3429267.

plain why specific legal norms were applied in a given case.[67] Similarly, judgments by the Voivodeship Administrative Courts often highlight that deficiencies in the justification constitute a significant violation of procedural law, which may lead to the annulment of an administrative decision. This approach strengthens procedural guarantees for citizens and enhances the transparency of public administration actions.[68]

The issue of justification in proceedings before an administrative court is repeatedly indicated in the administrative legislation. It appears here, among other reasons, for the application for the initiation of proceedings,[69] the reasons for the contested decision[70] or, finally, with the reasons for the judgment.[71] In jurisprudence, making it possible for all parties to understand the law, the courts state that there is a need to justify acts of public administration (here: regarding post-inspection orders)[72] or a fair analysis of the doubts raised by the complainant.[73]

National legislation also indicates the possibility of not justifying the decision. It is indicated that there is no need to justify a decision in which a party's request has been granted in full.[74] In addition, there is a possibility to waive the justification when in other temporary provisions such a possibility arises due to the interests of state security or public order.[75] Case-law indicates that despite the authority's reference to the interests of state security, the decision must contain a description of the factual and legal situation, and an evaluation and reasoning for refusal.[76]

Enforcement of the standards of the law is supervised by the Supreme Administrative Court, which resolves complaints concerning the decisions of the provincial administrative courts and clarifies the provisions about which there are discrepancies and doubts.[77] It must be clear from the appealed decision why a particular decision was refused, and that sometimes the authorities are not able to give a detailed justification due to "proprietary" documents.[78] The decision must not be implicit in the reasons and is one of the most important components of the decision.[79]

[67] Decision of the Supreme Administrative Court of January 28, 2011, II GSK 59/11, LEX no. 952852.

[68] Kmieciak, "Europejskie standardy prawa i postępowania administracyjnego a ustalenia orzecznictwa Naczelnego Sądu Administracyjnego."

[69] Art. 64 § 2, PPSA.

[70] Art. 54 § 2a, PPSA.

[71] Art. 141, PPSA.

[72] Judgment of the Provincial Administrative Court in Bialystok of November 22, 2017, II SA/Bk 587/17, LEX no. 2404113.

[73] Judgment of the Provincial Administrative Court in Bialystok of September 15, 2023, I SA/Bk 227/23, LEX no. 3612638.

[74] Art. 107 § 4, KPA.

[75] Art. 107 § 5, KPA.

[76] Judgment of the Provincial Administrative Court in Warsaw of April 28, 2022, VII SA/Wa 160/22, LEX no. 3360493.

[77] Art. 15, PPSA.

[78] Judgment of the Supreme Administrative Court of January 18, 2022, II OSK 1042/21, LEX no. 3288444 and Judgment of the Supreme Administrative Court of July 7, 2021, II OSK 3089/2, LEX no. 2002652.

[79] Judgment of the Supreme Administrative Court of January 18, 2022—Lodz Branch Center of July 18, 2019, I OSK 327/19, LEX no. 2778936.

Polish jurisprudence indicates that the Constitutional Court's invocation of the right to good administration, by referring to European sources of law, establishes that this right is a civil right that has its support in the Charter of Fundamental Rights,[80] in accordance with the judgment of the Constitutional Court of February 18, 2003, ref. K 24/02, OTK-A 2003/2/11, as well as in Recommendation CM/Rec(2007)7.[81] Also important is the reference in the justification to the Constitution of the Republic of Poland and the inherent and inalienable dignity of the human being, and the fact that its protection is the duty of public authorities.[82] By the above fact, it becomes the highest value due to every human being, which can be expressed by the authorities as the right to a fair trial.[83] Thus, it can be deduced that the justification of any rationale during the proceedings and decisions by the authority is a direct factor in maintaining the rule of law, which is contained in a fair trial.

One should also bear in mind the important judgment for Polish jurisprudence issued by the Supreme Administrative Court, which clearly indicates that the CJEU's jurisprudence has an overriding position to the administrative judiciary in Poland, and that Poland, as a member of the EU, must comply with its regulations.[84]

In the context of the growing use of new technologies in public administration, the issue of automatic generation of justifications for administrative decisions, especially using artificial intelligence tools, requires special attention. This process raises significant legal and ethical concerns, primarily with regard to the principle of transparency and the right to obtain an understandable justification for decisions that directly affect an individual's rights. According to Article 22 of the GDPR, an individual has the right not to be subject to a decision based solely on automated processing, including profiling, if it produces legal effects on him or similarly significantly affects him. The introduction of such solutions in public administration therefore requires not only strict adherence to EU regulations, but also ensuring that every decision—even if algorithm-assisted—has a rationale that is clear, understandable and contestable. Otherwise, basic standards of the rule of law, including the right to effective judicial protection, may be violated.[85]

[80] Art. 41, CFR.

[81] Judgment of the Provincial Administrative Court in Wroclaw of July 25, 2023, I SAB/Wr 140/23, LEX no. 3601828.

[82] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (consolidated text Journal of Laws of 2024, item 483 as amended).

[83] Judgment of the Provincial Administrative Court in Wroclaw of July 25, 2023, I SAB/Wr 140/23, LEX no. 3601828.

[84] Judgment of the Supreme Administrative Court of November 4, 2021, III FSK 4104/21, LEX no. 3309434.

[85] Sandra Wachter et al., "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law 7*, no. 2 (2017): 76–99, https://doi.org/10.1093/idpl/ipx005.

Summary

The article discusses the key aspects related to the obligation to justify administrative decisions in European and national law, particularly in the context of Poland. According to the case-law of the European Court of Justice, the justification of administrative decisions is a fundamental element of the right to effective judicial protection, ensuring transparency, fairness, and accountability in public administration. This highlights the necessity of adhering to the principles of good administration, such as the right to be heard, the right to access case files, and the obligation to justify decisions.

The European Convention on Human Rights also imposes on member states the obligation to protect individual rights, including the right to a fair trial, which in practice means that every administrative decision should include a justification that allows it to be understood and potentially challenged. Documents such as the Code of Good Administration and the ReNEUAL model regulations play an important role in setting guidelines for transparent and fair administrative procedures.

In the Polish legal system, the obligation to justify administrative decisions is derived from both national and European norms. Administrative courts, particularly the Supreme Administrative Court, play a crucial role in ensuring that administrative decisions are justified and comply with the law. As a member of the European Union and the Council of Europe, Poland is obligated to align its administrative law with international standards, which promotes consistency in laws and administrative procedures across member states.

The article also discusses the growing role of technology, particularly artificial intelligence (AI), in public administration. The use of AI in decision-making poses significant legal and ethical challenges, primarily concerning transparency and the right to obtain a clear justification for decisions affecting individual rights. The application of such technologies in public administration must comply with EU regulations, ensuring that every decision, even if assisted by algorithms, is well-reasoned, understandable, and contestable. Otherwise, basic rule of law standards, including the right to effective judicial protection, may be violated.

In conclusion, the justification of administrative decisions is crucial for maintaining the principles of the rule of law and ensuring fairness in public administration. Both European and national law impose a duty on public administration to be transparent and accountable, and administrative courts play a vital role in ensuring compliance with these principles.

BIBLIOGRAPHY

Craig, Paul. "Introduction to the ReNEUAL Model Rules / Book I—General Provisions." In *ReNEUAL Model Rules on EU Administrative Procedure*, edited by Herwig C.H. Hofmann, Jens-Peter Schneider, and Jacques Ziller. Research Network on EU Administrative Law, 2014.

Jaśkowska, Małgorzata. *Standardy współczesnej administracji i prawa administracyjnego*. Wolters Kluwer Polska, 2019.

Kmieciak, Zbigniew. "Europejskie standardy prawa i postępowania administracyjnego a ustalenia orzecznictwa Naczelnego Sądu Administracyjnego." *Ruch Prawniczy, Ekonomiczny i Socjologiczny* 60, no. 1 (1998): 51–60.

Krawiec, Grzegorz. "Europejskie standardy związane z przebiegiem postępowania administracyjnego." *Roczniki Administracji i Prawa*, no. 1 (2011): 69–85.

Princ, Marcin. *Standardy dobrej administracji w prawie administracyjnym*. Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza, 2016.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." *International Data Privacy Law* 7, no. 2 (2017): 76–99. https://doi.org/10.1093/idpl/ipx005.

Waldron, Jeremy. "Positivism and Legality: Hart's Equivocal Response to Fuller." *NYU Law Review* 83, no. 4 (2008): 1135–69.

Wronkowska, Sławomira, "Kilka tez o instrumentalizacji prawa i ochronie przed nią." *Przegląd Prawa i Administracji* 110, no. 3 (2017): 107–12. https://doi.org/10.19195/0137-1134.110.8.

Żak, Mariola. "Pojęcie standardu prawnego w sieciowym systemie prawa." *Przegląd Prawa Publicznego*, no. 1 (2019): 8–21.

ZESZYT PRAWNICZY UAM
NR 15/2025
https://doi.org/10.14746/zpuam.2025.15.4

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

JAKUB MARCINIAK

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0008-1919-477X
jakmar9@st.amu.edu.pl

Use of Artificial Intelligence Tools by Law Enforcement Services in Light of the Artificial Intelligence Act

Abstract: The purpose of the research of this text is to identify crimes for which law enforcement services can use real-time remote biometric identification systems in public spaces. This will be done by analysing the prerequisites that allow the use of this technology and comparing them to acts prohibited by the Polish Criminal Code. This results in the creation of a catalogue of crimes for which the services can use a real-time remote biometric identification system in public spaces. The findings of this research are very relevant due to the rapid development of artificial intelligence, which has been observed for several years.

Keywords: artificial intelligence, criminal law, cybersecurity, national security

Introduction

In the history of a humankind there are many turning points that separate different eras. One of such was the Industrial Revolution at the turn of the 18th and 19th centuries. Then, at the end of 20th century came the digital revolution with computers and telephones. Next step, which we may be eyewitnesses to is the development of artificial intelligence. Mastering fire, steam and heavy machines allowed us to produce substantially more goods, thereby helping our civilization to raise its standards; however, it also led to the environmental pollution that we are facing today. The increased processing power that came with computers helps disseminate information more easily, connecting with our beloved ones hundred miles away. Yet everyday internet access given to us by phones also came at a price in terms of many social issues. Entry into the world of artificial intelligence will probably also involve certain costs, although the nature of these costs is as yet unclear. However, it is imperative to prepare for this by providing relevant legal solutions. That was the motivation underpinning Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act),[1] which is widely known as the AI Act.

[1] OJ L, 2024/1689, 12.7.2024.

Acknowledging how powerful a tool artificial intelligence could be in the wrong hands, the legislative bodies of the European Union have limited the use of artificial intelligence in certain matters. One of these is "the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement," which is prohibited by Article 5(1)(h). However, there are some exceptions—according to the further part of this regulation, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement is possible for:

- (i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;
- (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;
- (iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

Therefore, it might be concluded that the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement is highly restricted and possible in only limited situations. The article seeks to identify the criminal offences listed in the Polish Criminal Code[2] for which the technology in question could be used, and then to propose solutions that would enable safer use of it. To rectify the above task, it is necessary to analyse the rationale for the law enforcement services' use of artificial intelligence, and then identify the prohibited acts listed by Polish legislation that implement this rationale. In answering the above question, the prerequisites use of the technology under discussion will be compared with the catalogue of criminal acts indicated in the PCC. A noteworthy fact is the significant differences between the various points of Article 5(1)(h): for this reason, each point will be considered separately.

It should be pointed out beforehand, however, that a regulation of the European Parliament and the Council of the European Union, unlike a directive, does not require implementation: it automatically becomes binding throughout the European Union from the date of its entry into force. This follows from Article 288 of the Treaty on the Functioning of the European Union. Moreover, it should be pointed out that Real-Time Remote Biometric Identification Systems in public spaces are technologies that enable automatic recognition of people's identities based on biometric characteristics (e.g., faces) without their knowledge or consent,

[2] Consolidated text Journal of Laws of 2025, item 383, hereinafter: PCC.

while moving in an open environment. They operate continuously, analysing data from surveillance cameras and comparing it with databases to identify specific individuals in real time.

1. Crimes Related to Article 5(1)(h)(i) of the AI Act

Point (i) relates to (only) victims of kidnapping, human trafficking and sexual harassment or searching for missing persons. While this regulation in no way relates to detection of offenders, it is clearly connected with some of crimes enlisted in PCC. Prohibited acts indicated in the PCC for which the law enforcement services may use remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement on the basis of Article 5(1)(h)(i) may be divided into three groups: human trafficking related crimes, sexual abuse-oriented crimes, and crimes against the care of minors.

The first of the above are prohibited by Article 189 and 189a of the PCC. This refers to unlawful deprivation of freedom, which is prohibited under the penalty of imprisonment for up to 5 years if the deprivation lasted for less then 7 days, up to 10 years if deprivation lasted for more then 7 days, up to 15 years if the deprivation involved a person who was unfit due to age, mental or physical condition, and finally up to 25 years if the deprivation was combined with special anguish. The subject of protection contained in this provision is freedom in the physical sense, which is understood as the ability to move and move freely.[3] Article 189a of the PCC refers to human trafficking and also list crimes where the law enforcement services can use artificial intelligence to search for victims. This is a relatively new regulation, having been added to the PCC in September 2010 as a result of ratification of Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children adopted by the United Nations General Assembly. The precise identification of the elements of this criminal act is facilitated by its definition in Article 115 § 22. According to this regulation, "human trafficking is recruiting, transporting, delivering, transferring, storing or receiving a person with the use of violence or unlawful threat, abductions, trickery, misrepresentation or exploitation of a mistake or inability to grasp the action taken, abuse of a relationship of dependence, taking advantage of a critical position or a state of helplessness, giving or accepting a pecuniary or personal benefit or the promise thereof to a person having custody or supervision of another person for the purpose of exploitation, even with her consent, in particular in prostitution, pornography or other forms of sexual exploitation, forced labour or services, begging, slavery or other forms

[3] Jerzy Lachowski, "Commentary on Article 189," in Arkadiusz Lach et al., *Kodeks karny: Komentarz* (LEX/el., 2023).

of exploitation degrading human dignity, or to obtain cells, tissues or organs in violation of the law."

Secondly, a considerably larger group of crimes that come under the regulation in question are crimes against sexual freedom and morality, which are regulated in Chapter XXV of the PCC. The most obvious example here is rape, which is prohibited under Article 197 § 1. Further paragraphs concern qualified forms of the same criminal act. It is noteworthy that this provision was recently amended by the law of June 28, 2024. This change has abolished the claim that there is no rape when resistance is apparent, which could be encountered before the aforementioned amendment.[4] Other criminal acts for which law enforcement services can use the 'real-time' remote biometric identification systems in publicly accessible spaces are:

- taking advantage of the vulnerability of another person or limited sanity, prohibited by Article 198;
- abusing a relationship of dependency or taking advantage of a critical situation, prohibited by Article 199;
- sexual intercourse with a minor, prohibited by Article 200;
- prohibition of establishing a connection with a minor, prohibited by Article 200a.

All of the above-mentioned crimes have similar characteristics: they are distinguished by the fact that the victims of the crimes indicated in them are people in a substantially weaker position than the person committing the sexual abuse. For this reason, Article 198 is designed to protect those unable to express legally relevant consent,[5] Article 199 is designed to protect those who are under the influence of an abuser (according to the Supreme Court jurisprudence, "the essence of a dependency relationship is that the dependent person is in such a relationship with the perpetrator that conflict with him threatens his material or immaterial interests"[6]), and Article 200 and Article 200a are designed to protect minors, i.e. persons whose sexuality is subject to special protection under the law.

The last criminal act that fulfils the prerequisites referred to in Article 5(1)(h)(i) is the abduction of a minor or a person who is helpless, as prohibited by Article 211. According to this regulation, it is prohibited to abduct a minor younger than 15 years old or a person who is unfit due to their mental or physical condition against the will of the legal guardian. Article 211 is intended to protect a state of proper care given to a minor or a person who is unfit due to their mental or physical con-

[4] Marek Mozgawa, "Commentary on Article 197," in Magdalena Budyn-Kulik et al., *Kodeks karny: Komentarz aktualizowany* (LEX/el., 2025).

[5] Piotr Zakrzewski, "Commentary on Article 198," in Adam Błachnio et al., *Kodeks karny: Komentarz* (LEX/el., 2024).

[6] Judgement of Supreme Court of Republic of Poland of May 6, 2014, V KK 358/13, LEX no. 1482486.

dition by it's legal guardian.[7] The Polish Supreme Court has even pointed that the subject of legal protection under this provision is not the freedom of the abducted or detained person.[8] It is a crime prosecuted by public indictment,[9] which is of great importance, considering the article's subject matter: law enforcement bodies don not require the initiative of the victim.

In concluding the discussion of point (i), it should be emphasized once again that the use of a 'real-time' remote biometric identification systems in publicly accessible spaces in the law enforcement services' action against the above-mentioned crimes is possible only for the purposes of a targeted search for specific victims.

2. Crimes Related to Article 5(1)(h)(ii) of the AI Act

The next section of the provision in question contains a much broader catalogue of criminal acts for which law enforcement services may use 'real-time' remote biometric identification systems in publicly accessible spaces. This is due to the use of vague (in the sense of Polish criminal law) expressions—"the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack." Far less questionable are the offences contained in the second part of the quoted passage, thus the analysis will begin with this article.

The PCC contains three prohibited acts directly related to terrorism—bringing in conditions that are universally dangerous to life or health prohibited by Article 165, financing terrorist activity prohibited by Article 165a, and placing a dangerous device or substance on a ship or in a public land transport facility prohibited by Article 167. However, one of these articles allows for a significant expansion of this set. According to Article 165a § 1, "whoever collects, transfers or offers means of payment, financial instruments, securities, foreign exchange, property rights or other movable or immovable property with the intent to finance a terrorist offence or an offence referred to in Article 120, Article 121, Article 136, Article 166, Article 167, Article 171, Article 252, Article 255a or Article 259a"—thus, if one considers the act prohibited by Article 165a to be a terrorist threat, as referred to in the Article 5(1)(h)(ii), the consequence will be that use of a 'real-time' remote biometric identification systems in publicly accessible spaces may also be possible in cases of acts prohibited by Article 120, Article 121, Article 136, Article 166, Article 167, Article 171, Article 252, Article 255a or Article 259a. Such an interpretation of the cited provision of the ordinance greatly expands the possibilities of law enforcement services as to the technology in question.

[7] Marek Mozgawa, "Commentary on Article 211," in Budyn-Kulik et al., *Kodeks karny*.

[8] Judgement of Supreme Court of Republic of Poland of December, 18, 1992, I KZP 40/92, LEX no. 22106.

[9] Julia Kosonoga-Zygmunt, "Commentary on Article 211," in Błachnio et al., *Kodeks karny*.

Moreover, the PCC contains a definition of a terrorist act: according to Article 115 § 20, "A terrorist offence is a prohibited act with a sentence of imprisonment for at least five years, committed with the aim of: 1) seriously terrorising a large number of people, 2) forcing a public authority of the Republic of Poland, or another state or international organisation, to take or not to take a certain course of action, 3) cause a serious disturbance in the political system or the economy of the Republic of Poland, or another state or international organisation,- or a threat to commit such an act." Analysing this provision, one must come to the conclusion that the Polish legislator abandoned the concept of including an act of terrorism in the framework of a specific criminal act in favour of the possibility of qualifying almost any criminal act (as long as it is punishable by imprisonment, the upper limit of which is at least 5 years—this is the only strict condition under the cited definition) as an act of terrorism due to the intended effect of the criminal. As indicated in the literature, the commission of a terrorist offence is an extraordinary aggravating circumstance under criminal law, as well as an element of certain criminal acts.[10] It is therefore impossible to identify all criminal acts for which it is possible for law enforcement to use 'real-time' remote biometric identification systems in publicly accessible spaces. The legality of the use of such an instrument should be considered on a case-by-case basis, taking into account Article 115 § 20.

An even more complicated issue is the creation of a catalogue of legitimate uses of the technology in question, based on the first part of the Article 5(1)(h)(ii). The expression "the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons" naturally refers to Chapter XIX of the PCC—Crimes against life and health. Hence, it can be pointed out that counteracting the crimes indicated in Article 148, Article 148a, Article 149, Article 150, Article 151, Article 152, Article 153, Article 154, Article 155, Article 156, Article 156a, Article 157, Article 157a, Article 158, Article 159, Article 160, Article 161, and Article 162 qualifies as an action referred to in the Article 5(1)(h)(ii). Nevertheless, in other parts of the PCC, you can also find criminal acts that meet the premise of the "threat to the life or physical safety of natural persons," despite the fact that the legally protected good is not human life and health as is the case with the aforementioned regulations. The following can be indicated as examples of such: Article 117, Article 118, Article 118a, Article 120, Article 121, Article 123, Article 134, Article 135, Article 136, Article 163, Article 164, Article 165, Article 166, Article 167, Article 171, Article 172, Article 173, and Article 223. Discussing each of the aforementioned provisions is a task far beyond the scope of this work; therefore, suffice to say, although the object of protection of the crimes specified in these provisions is not always human

[10] Michał Grudecki, "Commentary on Article 115," in Jan Kulesza et al., *Kodeks karny: Komentarz* (LEX/el., 2025).

health and life, the consequence of such crimes as those against peace or humanity, and war crimes or crimes against public safety will always be the endangerment of human life or the safety of individuals. In view of the above, in the opinion of the author of this text, the way in which the provision in question is drafted is far from optimal, as it may give rise to many doubts of interpretation in practice.

Once again, however, it should be pointed out that the use of a 'real-time' remote biometric identification systems in publicly accessible spaces in the struggle of the law enforcement services against the above-mentioned crimes is possible only for the purpose of prevention.

3. Crimes Related to Article 5(1)(h)(iii) of the AI Act

The last of the points justifying the use of a 'real-time' remote biometric identification systems in publicly accessible spaces is the most specific of the three, as it refers to one of the annexes to the regulation, which contains a catalogue of crimes. Annex II lists the following crimes:

- terrorism,
- trafficking in human beings,
- sexual exploitation of children, and child pornography,
- illicit trafficking in narcotic drugs or psychotropic substances,
- illicit trafficking in weapons, munitions or explosives,
- murder, grievous bodily injury,
- illicit trade in human organs or tissue,
- illicit trafficking in nuclear or radioactive materials,
- kidnapping, illegal restraint or hostage-taking,
- crimes within the jurisdiction of the International Criminal Court,
- unlawful seizure of aircraft or ships,
- rape,
- environmental crime,
- organised or armed robbery,
- sabotage,
- participation in a criminal organisation involved in one or more of the offences listed above.

Many of those crimes were mentioned previously but in a different context–it should be noted once more that only point (iii) allows law enforcement services to use 'real-time' remote biometric identification systems in publicly accessible spaces against offenders, to search for offenders. However, in indicating the specific provisions of the PCC that sanction the crimes indicated in the annex in question, it should be pointed out that the crimes indicated therein often correspond to several provisions of the criminal act.

Starting the consideration of the crimes indicated in the catalogue with terrorism, it has already been mentioned that Articles 165, 165a and 167 can certainly qualify here. A consequence of the qualification of Article 165a may also be the recognition that law enforcement can take advantage of the tools offered by artificial intelligence in the fight against offenders of crimes sanctioned by Article 120, Article 121, Article 136, Article 166, Article 167, Article 171, Article 252, Article 255a, or Article 259a. An even more complicated issue is that the vast majority of crimes can be considered an act of terrorism under the definition under Article 115 § 20 as long as it was intended to produce a specific effect referred to in the provision. Another in the catalogue of crimes is human trafficking, which is defined by Article 115 § 22 and prohibited by Article 189a. When it comes to sexual exploitation of children and child pornography, we may point crimes prohibited by Article 197 § 4, Article 200, Article 200a and Article 200b. Another crime listed in the catalogue in question is illicit trafficking in narcotic drugs or psychotropic substances. Interestingly, the PCC does not refer to this crime–it is prohibited under Article 55, Article 56, Article 58 and Article 59 of the Law on Counteracting Drug Addiction, which is a separate act regulating drugs and other psychoactive substances, including criminal issues. The next crime is illicit trafficking in weapons, munitions or explosives, as prohibited by Article 171 and Article 263. Crimes such as murder and grievous bodily injury correspond to Article 148, Article 156 and Article 158 in the Criminal Code. A rather unusual crime is illicit trafficking in nuclear or radioactive materials, which is prohibited by Article 171. Kidnapping, illegal restraint or hostage-taking were also partly discussed: in this respect, this concerns regulations such as Article 189, Article 211 and Article 252. Complications stem from crimes within the jurisdiction of the International Criminal Court; in order to identify the provisions of the Code covering these crimes, reference should be made to the Rome Statute of the International Criminal Court. In accordance with Article 5 of the same act, the Court's jurisdiction under this statute shall include the following crimes: genocide, crime against humanity, war crime of aggression. These are defined in the following provisions: Article 6, Article 7 and Article 8. Those crimes are also prohibited by the PCC—Article 117, Article 118, Article 118a, Article 120, Article 122 and Article 123. The crime of unlawful seizure of aircraft or ships is prohibited by Article 166. Rape, which was also previously discussed, is regulated by Article 197. Environmental crime is a very broad term: in the PCC, this issue is given a separate chapter. For this reason, the crime against the environment is prohibited by Article 181, Article 182, Article 183, Article 184, Article 186, Article 187 and Article 188. Use of a 'real-time' remote biometric identification systems in publicly accessible spaces against offenders by law enforcement services is also legal when it comes to qualified forms of robbery. This relates to armed robbery regulated by Article 280 § 2 or organised robbery, which may be qualified as a crime that violates Article 258, which concerns a much broader category than robbery, namely, the activities of

organized criminal activity. In terms of the crime of sabotage, it should be pointed out that the word occurs only once in the Criminal Code—in Article 130 § 7, which deals with the broader crime of espionage. The last type of crime listed in the catalogue found in Annex 2 to the regulation in question is participation in a criminal organisation involved in one or more of the offences listed above. Participation in an organized criminal group is regulated in Article 258 of the Criminal Code, but participation alone is insufficient for law enforcement to be authorized to use the 'real-time' remote biometric identification systems in publicly accessible spaces. The objects of these groups must be crimes on the list in question.

4. Other Limitations of Use of Artificial Intelligence Tools by Law Enforcement Services

However, the cases mentioned in the above paragraphs are subject to additional restrictions, which are indicated in the paragraphs of Article 5. As stated in paragraph 2, "the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), shall be deployed for the purposes set out in that point only to confirm the identity of the specifically targeted individual." The same provision indicates that the decision to use the technology in question should be made taking into account (a) "the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm that would be caused if the system were not used" and (b) "the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences." While the principle of using these systems only against a wanted person undoubtedly increases the security of its use, the indications in points a and b are expressed in vague language. Consequently, it is difficult to state whether they will actually help reduce potential abuse. It is noteworthy noting that a further part of the provision also requires law enforcement to register the system it uses in the relevant European Union database to be established under Article 49. However, the most important issue is addressed in paragraph 3—in order to use 'real-time' remote biometric identification system in publicly accessible spaces, it is necessary to obtain "a prior authorisation granted by a judicial authority or an independent administrative authority whose decision is binding of the Member State." The use of these systems without a previously obtained permit will be possible only in exceptional cases, but even then the application for a follow-up permit should be submitted within 24 hours after use. The issue of establishing regulations clarifying the use of this technology is largely left to national legislatures by the regulation—"Member States concerned shall lay down in their national law the necessary detailed rules for the request, issuance and exercise

of. Regardless of the permit issued, in accordance with paragraph 6, each use of a 'real-time' remote biometric identification system in publicly accessible spaces for law enforcement purposes shall be notified to the relevant market surveillance authority and the national data protection authority." These bodies report annually to the European Commission on the use of this technology in a form prepared by the European Commission. The need for the relevant state authority to report annually on the use of use the 'real-time' remote biometric identification systems in publicly accessible spaces is, at first glance, not a major limitation. However, with the increased use of this technology and, therefore, the experience of the courts and the administration, the creation of a centralised database on the use of this technology will enable more effective control and revision of this regulation to adapt to law enforcement practice.

Despite the above restrictions from the content of the regulation, member states may restrict the use of the technology in question on their own—"Member States may introduce, in accordance with Union law, more restrictive laws on the use of remote biometric identification systems."

Summary

Having made a brief analysis of all three points in Article 5(1)(h), it should be pointed out that the scope of crimes for which it is possible to use the 'real-time' remote biometric identification systems in publicly accessible spaces exceptionally wide. The regulation in question, while limiting the use of this controversial technology, establishes a very extensive system of "exceptions" in which it is possible. Thus, without considering whether law enforcement agencies use the tools offered by artificial intelligence to search for victims, prevent crimes, or locate and identify suspected offenders, it can be concluded that the use of 'real-time' remote biometric identification systems in publicly accessible spaces when dealing with acts criminalized by the following articles of PCC: 117, 118, 118a, 120, 121, 122, 123, 130, 134, 135, 136, 148, 149, 150, 151, 152, 153, 154, 155, 156, 156a, 157, 158, 159, 160, 161, 162, 163, 164, 165, 165a, 166, 167, 171, 172, 173, 181, 182, 183, 184, 186, 187, 188, 189, 189a 197, 198, 199, 200, 200a, 211, 223, 252, 255a, 258, 259a, 263, 280. Not to be forgotten, of course, are articles 55, 56, 58 and 58 of Law on Counteracting Drug Addiction. Furthermore, given the content of Article 115(20), which defines a terrorist crime by the intent of the offender, the catalogue is significantly expanded.

Although the above-created catalogue of criminal acts may, at first glance, overwhelm with its volume and raise doubts about the actual limitation of this very powerful technology, it should be noted that all of the above crimes are undoubtedly extremely serious. Therefore, it is to be hoped that law enforcement agencies will

use the tools given to them wisely and prevent numerous crimes, at the same time without bending the norms of the ordinance in question formulated in imprecise language, which could undoubtedly prove tragic for civil and human rights. Combined with the necessity of obtaining a permit issued by the judiciary in each case and the need to report to the designated authorities, it seems that this regulation will effectively protect citizens of the European Union while not unduly restricting the possibility of fighting crimes by the services established for this purpose.

In the opinion of the author of this text, it would be reasonable to introduce our own national rules on the use of 'real-time' remote biometric identification systems in publicly accessible spaces. Such a solution, facilitated by the norm expressed in Article 5(1) of the AI Act, would make it possible to adapt EU regulations to the Polish criminal law system, which would effectively eliminate the problems of interpretation that arise, for example, in the case of terrorism. Given the power of the technology in question and the threat posed by its misuse by law enforcement, this appears to be a solution that could effectively secure the privacy of citizens.

BIBLIOGRAPHY

Grudecki, Michał. "Commentary on Article 115." In Jan Kulesza, Adam Behan, Mateusz Filipczak, Michał Grudecki, Krystyna Patora, and Krzysztof Wala, *Kodeks karny: Komentarz*, LEX/el., 2025.

Kosonoga-Zygmunt, Julia. "Commentary on Article 211." In Adam Błachnio, Julia Kosonoga-Zygmunt, Jarosław Majewski, and Piotr Zakrzewski, *Kodeks karny: Komentarz*. LEX/el., 2024.

Lachowski, Jerzy. "Commentary on Article 189." In Arkadiusz Lach, Jerzy Lachowski, Tomasz Oczkowski, Igor Zgoliński, and Agata Ziółkowska, *Kodeks karny: Komentarz*. LEX/el., 2023.

Mozgawa, Marek. "Commentary on Article 197." In Magdalena Budyn-Kulik, Patrycja Kozłowska-Kalisz, Marek Kulik, and Marek Mozgawa, *Kodeks karny: Komentarz aktualizowany*. LEX/el., 2025.

Mozgawa, Marek. "Commentary on Article 211." In Magdalena Budyn-Kulik, Patrycja Kozłowska-Kalisz, Marek Kulik, and Marek Mozgawa, *Kodeks karny: Komentarz aktualizowany*, LEX/el., 2025.

Zakrzewski, Piotr. "Commentary on Article 198." In Adam Błachnio, Julia Kosonoga-Zygmunt, Jarosław Majewski, and Piotr Zakrzewski, *Kodeks karny: Komentarz*. LEX/el., 2024.

ZESZYT PRAWNICZY UAM
NR 15/2025
https://doi.org/10.14746/zpuam.2025.15.5

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

KAMILA MORAWIEC

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0004-1393-5232
kammor1@st.amu.edu.pl

MAJA PRZYBYLAK

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0005-2046-2522
majprz4@st.amu.edu.pl

The Right to Life and the Right to Die—Legal and Ethical Considerations Based on the Jurisprudence of the European Court of Human Rights

Abstract: The right to die is a strongly debated issue in both law and ethics. While the European Convention on Human Rights does not explicitly guarantee it, the European Court of Human Rights (ECtHR) examines it in the context of the right to life, the prohibition of torture, and the right to privacy. This paper analyses the ECtHR case-law on euthanasia, assisted suicide, and the withdrawal of life-sustaining treatment, presenting arguments from both applicants and the ECtHR. It also explores the state's role in protecting life and the absence of a clear obligation to guarantee the right to die. Special attention is given to access to legal procedures for euthanasia requests and medications for assisted suicide, as well as the resulting positive obligations of the state.

Keywords: euthanasia, assisted suicide, ECtHR case-law, the right to death

Introduction

The right to life, regulated in Article 2 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter: the Convention), is the most fundamental of all guaranteed rights. Undoubtedly, human life is a primary value protected by law, as without ensuring the right to life, the effectiveness of any other subjective right is difficult to uphold. Without guaranteeing the protection of life and existence, one cannot fully enjoy rights such as the right to liberty or the right to respect for private and family life. Article 2 of the Convention states that "everyone's right to life shall be protected by law" and also enumerates situations in which "deprivation of life shall not be regarded as inflicted in contravention of this Article."[1]

While the existence and significance of the right to life are beyond dispute, determining its precise scope remains problematic. This issue arises particularly in the context of the concept of the right to die. Questions emerge as to whether the Convention guarantees a right to die at all. If so, does it stem from Article 2 of the Convention, or perhaps from Article 3, which establishes the prohibition of torture

[1] Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, (consolidated text Journal of Laws of 1993, item 284).

and inhuman treatment, or from Article 8, which guarantees the right to respect for private and family life?

This article attempts to answer the questions posed above. To this end, an analysis has been conducted of the case-law of the European Court of Human Rights (hereinafter: ECtHR) related to the concept of the right to die. The selected rulings primarily address cases concerning active euthanasia, passive euthanasia, and assisted suicide.

1. Active Euthanasia

First, it is necessary to define and distinguish active euthanasia from passive euthanasia. One of the proposed distinctions states that active euthanasia occurs when an external action directly causes a patient's death, such as administering a lethal substance. In contrast, passive euthanasia takes place when life is allowed to end by withholding or withdrawing medical interventions that were previously initiated by a physician. According to this distinction, removing a respirator from a patient is considered passive euthanasia, while administering even a small dose of poison to a weakened patient qualifies as active euthanasia. The key factors differentiating the two include the causal role of the action and the patient's treatment history, specifically, whether a medical measure was initially introduced to counteract the progression of the illness and is later withdrawn.[2]

Legal regulations regarding active euthanasia vary around the world. Currently, European countries stand out in terms of access to active euthanasia—in the Netherlands, Belgium, and Luxembourg, active euthanasia is legal, although even within these countries the regulations differ significantly. For example, in the Netherlands, both active euthanasia and physician-assisted suicide are legal, while Belgium only regulates active euthanasia. The Netherlands allows patients from age 12 to 18 to request active euthanasia, while Belgium does not have provisions for minors. In Belgium, a second doctor must be consulted if the patient is not terminally ill, unlike the Netherlands, where a second consultation is not required for non-terminal cases.[3]

By contrast, active euthanasia is entirely illegal in Poland. In this context, it is worth mentioning the offence of euthanatic homicide under Article 150 of the Polish Penal Code.[4] This provision states that killing a person at their request and out of compassion is punishable by imprisonment for a period ranging from 3

[2] Bernward Gesang, "Passive and Active Euthanasia: What Is the Difference?," *Medicine, Health Care Philosophy* 11, no. 2 (2008): 177–78, https://doi.org/10.1007/s11019-007-9087-x.

[3] Luc Deliens and Gerrit Van der Wal, "The Euthanasia Law in Belgium and the Netherlands," *The Lancet* 362, no. 9391 (2003): 1239–40, https://doi.org/10.1016/S0140-6736(03)14520-5.

[4] Ustawa z dnia 6 czerwca 1997 r.—Kodeks karny (consolidated text Journal of Laws of 1997, item 553 as amended).

months to 5 years. However, in exceptional cases, the court may apply extraordinary mitigation of punishment or even refrain from imposing a sentence. This variation in the legality of active euthanasia among European countries, including Member States of the Council of Europe, clearly demonstrates that no European consensus has emerged on this issue.

In the case of *Mortier v. Belgium*, the ECtHR had, for the first time, the opportunity to examine a case concerning active euthanasia and the nature of states' obligations under Article 2 of the Convention, taking into account domestic law permitting euthanasia.[5] The case was introduced by a son of a person who died by euthanasia. The applicant's mother, G.T., had suffered from chronic depression for 40 years. G.T. sought euthanasia due to her long-term mental suffering and the failure of all other treatment options. After consultations with multiple doctors, including psychiatrists, her request was ultimately approved under Belgium's Euthanasia Act. G.T. informed her daughter and the applicant, Mr. Mortier, of her intention to undergo euthanasia but did not wish to involve them further in the process, which resulted in Mr. Mortier learning about his mother's death only a day after the procedure had been carried out.

The applicant raised allegations under Articles 2 and 8 of the Convention, complaining that the statutory framework did not afford an effective safeguard for protecting vulnerable individuals' right to life, as his mother was able to change doctors until she found one willing to perform euthanasia. Mr. Mortier also highlighted a conflict of interest, as the doctor who carried out the procedure only agreed to do so after receiving a €2,500 donation to the LEIF association, which he chaired. The applicant also argued that the Euthanasia Act had not been properly followed, as his mother was not in a hopeless medical situation, her suffering could have been alleviated, and the consulted doctors were not independent. Additionally, no discussion took place with her regular medical team, rendering safeguards insufficient. Finally, Mr. Mortier argued that the investigation into his mother's euthanasia lacked independence and was ineffective.

The Government of Belgium argued that the applicant's mother's right to life had been respected, emphasizing the state's wide margin of appreciation in end-of-life matters, as there was no consensus among the Member States on the issue of euthanasia. The Government contended that conditional decriminalization of euthanasia was permissible under the ECtHR's case-law, provided strict conditions and oversight mechanisms were in place. The Government maintained that Belgium's Euthanasia Act ensured voluntary euthanasia with safeguards, confidentiality obligations for doctors, an independent review process, and no prosecutorial immunity, while also asserting that the LEIF association served the public interest and that the reopened 2019 investigation was effective, preventing any procedural violation of Article 2.

[5] Judgement of the ECtHR of October 4, 2022, *Mortier v. Belgium*, application no. 78017/17.

The ECtHR emphasized that end-of-life matters, particularly euthanasia, raise complex legal, social, moral and ethical issues, with significant differences in how Member States approach them. Therefore, while these states have a margin of appreciation in striking a balance between the right to life with personal autonomy, this discretion is not unlimited, and the ECtHR retains the authority to review compliance with Article 2.[6]

After examining whether Belgium's Euthanasia Act provided effective safeguards and whether the applicant's mother's euthanasia complied with Article 2, the ECtHR found that there was no violation of the right to life as the Act ensured voluntary decisions with procedural safeguards, especially in cases of mental suffering. The euthanasia process in this case followed legal requirements, with independent medical assessments. On the other hand, the ECtHR found that the State had failed to fulfil its procedural positive obligation on account of the lack of independence of the Board—the federal administrative body that was in charge of reviewing and assessing euthanasic procedures—and of the length of the criminal investigation in the present case, resulting in the violation of Article 2 of the Convention. Lastly, the ECtHR found no violation of Article 8 of the Convention in regard to the applicant's claims, particularly concerning the conduct of the doctors involved in the euthanasia. It acknowledged the doctors' professional obligations, including their duty of confidentiality and medical secrecy, as well as their efforts to persuade the applicant's mother to inform her children about her intention to undergo euthanasia. Despite these efforts being unsuccessful, the ECtHR concluded that the balance between the applicant's right to family life and the mother's autonomy was properly struck by the national legislation, and no breach of Article 8 occurred.

Most importantly, in the judgment under review, the ECtHR emphasized that it is not possible to derive a right to die from Article 2 of the Convention, yet the right to life guaranteed by this article should not be understood as prohibiting the conditional decriminalization of euthanasia.[7] Furthermore, the ECtHR also highlighted that the decriminalization of euthanasia in accordance with Article 2 of the Convention must be accompanied by adequate and sufficient safeguards to prevent abuses and ensure respect for the right to life. To this end, the ECtHR referred to the views of the United Nations Human Rights Committee, stressing that these safeguards should ensure that doctors adhere to the patient's clear, unequivocal, voluntary, and informed decision, thus protecting them from pressure and abuse.[8]

Another case examined by the ECtHR concerning, *inter alia*, active euthanasia was the case of *Dániel Karsai v. Hungary*.[9] Mr. Karsai was an outstanding lawyer specializing in constitutional law and human rights. At the age of 47, in 2024, he

[6] Judgement of the ECtHR of October 4, 2022, *Mortier v. Belgium*, §§ 142–43.
[7] Judgement of the ECtHR of October 4, 2022, *Mortier v. Belgium*, § 138.
[8] Judgement of the ECtHR of October 4, 2022, *Mortier v. Belgium*, § 139.
[9] Judgement of the ECtHR of September 9, 2024, *Dániel Karsai v. Hungary*, application no. 32312/23.

passed away due to amyotrophic lateral sclerosis (ALS). ALS is a progressive neurodegenerative disease that leads to the gradual loss of motor functions and ultimately results in fatal respiratory paralysis. Despite intact sensory and cognitive abilities, there is no effective treatment, and care focuses on symptom management, with death typically occurring within three to five years. The applicant first showed symptoms of the disease in 2021, and his condition rapidly deteriorated in 2023, resulting in his death on 28 September 2024.[10]

Mr. Karsai lodged a complaint with the ECtHR under Article 8 of the Convention, arguing that Hungarian law did not allow him to end his life with assistance, in breach of his right to private life. In this case, ending life with assistance was defined as physician-assisted dying (hereinafter: PAD), which includes assisted suicide and voluntary euthanasia when carried out in a regulated and medically supervised setting, as well as the refusal (by the patient) or withdrawal (at the patient's request) of life-sustaining or life-saving interventions, such as respiratory support, ultimately leading to the patient's death.[11]

The ECtHR observed that due to Mr. Karsai's medical condition, the applicant had no real possibility of ending his life on his own terms. This not only fell within the scope of Article 8 of the Convention but also constituted an interference with his right to private life. The ECtHR considered that this case concerns the core of the right to private life, as it concerns respect for his autonomy, physical and mental integrity and for human dignity, which lies in the very essence of the Convention.[12] Furthermore, the ECtHR emphasized the broad margin of appreciation afforded to Member States in regulating matters related to assisted dying, particularly in light of the lack of European consensus on the issue. However, it was noted by the ECtHR that in some Member States, such as Austria, Germany, and Spain, some important legal developments in favour of granting some form of access to PAD have occurred over last few years. Despite this emerging trend, the majority of states continued to criminalize PAD and international law did not impose an obligation to legalize such practices. Given these considerations, the ECtHR concluded that Hungary's absolute prohibition of PAD fell within the state's margin of appreciation and did not violate Article 8 of the Convention.[13]

Judge Wojtyczek submitted a partly concurring, partly dissenting opinion on the aforementioned judgment.[14] He challenged the ECtHR's reasoning in the part where, following rulings such as *Mortier v. Belgium*, it found that Article 2 of the

[10] Judit Sandor, "A Lawyer's Legacy: The Significance of the *Dániel Karsai V. Hungary* Case," *Pravni Zapiši* 15, no. 3 (2024): 311–12.

[11] Judgement of the ECtHR of September 9, 2024, *Dániel Karsai v. Hungary*.

[12] Judgement of the ECtHR of September 9, 2024, *Dániel Karsai v. Hungary*, § 85.

[13] Judgement of the ECtHR of September 9, 2024, *Dániel Karsai v. Hungary*, § 166.

[14] Krzysztof Wojtyczek, "Partly Concurring, Partly Dissenting Opinion of Judge Wojtyczek," *Dániel Karsai v. Hungary*.

Convention does not preclude domestic law from allowing euthanasia. In his opinion, Judge Wojtyczek advocated for a strict interpretation of Article 2, arguing that the four exceptions to the prohibition of the intentional deprivation of life enumerated in the provision cannot be expanded. These exceptions-namely, the execution of a court sentence imposing the death penalty for a crime punishable by law, the defence of any person from unlawful violence, the lawful arrest or prevention of escape of a person lawfully detained, and actions taken in accordance with the law to quell a riot or insurrection[15]—do not include an exception for euthanasia or medically assisted suicide. This led to the conclusion that the right to life guaranteed by Article 2 of the Convention cannot be interpreted as allowing an additional exception in the form of PAD. Furthermore, Judge Wojtyczek disagreed with the majority's finding that physician-assisted dying falls within the scope of private life under Article 8, asserting instead that the request for PAD pertains to the right to life.

The aforementioned judgments of the ECtHR, namely *Mortier v. Belgium* and *Karsai v. Hungary*, clearly demonstrate that the right to death in the form of access to active euthanasia cannot be derived from either Article 2 of the Convention, which guarantees the right to life, or Article 8, which guarantees the right to privacy, including respect for individual autonomy and physical and mental integrity. These rulings also highlight the wide margin of appreciation granted to Member States regarding end-of-life decisions, indicating that the Convention does not preclude domestic regulations allowing active euthanasia. However, the applicant's arguments, as well as the partly concurring, partly dissenting opinion of Judge Wojtyczek, illustrate that in the legal and especially ethical sense, this issue remains far from settled, and the scope and interpretation of the right to life and the right to privacy in the context of the right to die continue to raise concerns.

2. Passive Euthanasia

The ethical and legal debate surrounding passive euthanasia, which includes cessation of therapy, raises profound questions about personal autonomy, medical responsibility, and state obligations in this matter. Unlike active euthanasia, it allows death to occur naturally by stopping interventions that prolong suffering without benefit. Advocates argue it respects patient's autonomy and dignity, while opponents fear it undermines the duty to preserve life.

While Article 2 of the Convention guarantees the protection of life, the ECtHR acknowledged that in certain cases withdrawing life-sustaining treatment does not constitute a violation of this right. Instead, it falls within the scope of medical

[15] Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950.

ethics and national discretion, as seen in landmark rulings such as *Lambert and Others v. France*.[16]

Passive euthanasia, defined as a withdrawal or withholding of life-prolonging treatment,[17] differs fundamentally from active euthanasia, where medical intervention directly causes death. Passive euthanasia as a result of deliberate withholding or withdrawal of life-sustaining medical treatments, allows a terminally ill or irreversibly unconscious patient to die naturally from their underlying condition. It involves omitting medical interventions such as mechanical ventilation or artificial nutrition and hydration, when such treatments are deemed medically futile, burdensome, or contrary to the patient's wishes. Similarly, the cessation of therapy refers to the discontinuation of treatments deemed non-beneficial or disproportionate to the patient's condition.[18] This practice is legally and ethically complex, balancing between respecting patient's autonomy under Article 8 of the Convention (right to private life) and the state's duty to safeguard life. As medical advancements prolong life beyond natural limits, societies must confront the question: does the right to live inherently include the right to die?

The legal status of passive euthanasia varies across European countries, depending on different ethical and legal perspectives on the end-of-life issue. For instance, in Germany and Finland passive euthanasia—in cases of terminal illness or medical futility—is legally permitted, whereas active euthanasia is illegal in these countries. On the other hand, the Netherlands, Belgium, and Luxembourg, allow both passive and active euthanasia under regulated circumstances. Meanwhile, in the United Kingdom and France, euthanasia is prohibited entirely. However, terminal patients in France can request to be heavily sedated until they die. As already mentioned, Poland has a stricter policy, concerning euthanasia to be a crime that is regulated in Article 150 of the Polish Penal Code. In light of these regulations, it appears to be difficult to distinguish between active euthanasia and withdrawal of life-sustaining treatment.[19]

In spite of these differences amongst European countries, the ECtHR has ruled in cases such as *Lambert and Others v. France* that the decision to withdraw life-sustaining treatment falls within a state's "margin of appreciation", which allows each country to regulate passive euthanasia according to its own legal framework. This legal diversity highlights the ongoing debate and lack of consensus between protecting life and respecting patients' autonomy across Europe. The ECtHR's ruling

[16] Judgement of the ECtHR of June 13, 2024, *Lambert and Others v. France*, application no. 46043/14.

[17] Iain Brassington, "What Passive Euthanasia Is," *BMC Medical Ethics* 21, no. 41 (2020): 3–6, https://doi.org/10.1186/s12910-020-00481-7.

[18] Eve Garrard and Stephen Wilkinson, "Passive Euthanasia," *Journal of Medical Ethics* 31, no. 1 (2024): 64–68, https://doi.org/10.1136/jme.2003.005777.

[19] Marcin Śliwka and Aneta Gałęska-Śliwka, "Regulating End of Life Decisions in Poland: Legal Dilemmas," *Advances in Palliative Medicine* 10, no. 2 (2021): 49–56.

in *Lambert and Others v. France* marked a significant decision on end-of-life care, affirming that the withdrawal of life-sustaining treatment does not violate the right to life.

This case concerned Vincent Lambert, who was in a vegetative state, with no signs indicating a minimally conscious state.[20] His family was divided over whether to continue artificial nutrition and hydration or cease it. They contended that ending Mr. Lambert's life by withdrawing treatment amounted to a breach of the state's obligation to protect life. They argued that depriving him of nutrition and hydration would constitute ill-treatment amounting to torture within the meaning of Article 3 of the Convention. They further argued that the lack of physiotherapy and the lack of therapy to restore the swallowing reflex amounted to inhuman and degrading treatment in breach of that provision. Furthermore, they submitted that the withdrawal of nutrition and hydration would also infringe Mr. Lambert's physical integrity, in breach of Article 8 of the Convention. Lastly, they argued that the French legal framework lacked sufficient safeguards, making it too easy to end life-sustaining treatment.[21]

The ECtHR ruled that the withdrawal of artificial nutrition and hydration from Mr. Vincent Lambert did not violate the right to life, emphasizing that states enjoy a margin of appreciation in regulating end-of-life decisions and that the right to life does not impose an absolute duty to prolong life in all circumstances.[22] Given that French law provided clear legal safeguards, including medical assessments and judicial oversight, the ECtHR assessed no violation of Lambert's rights.[23] It also ruled that the right to private and family life was not breached, as the legal process had properly considered Lambert's presumed wishes, medical opinions, and the views of his family.[24] This decision reinforced the legality of passive euthanasia, affirming that withdrawing life-sustaining treatment can be lawful when based on medical necessity and appropriate legal safeguards.

The legal and ethical debate on passive euthanasia remains complex, balancing patient autonomy and the state's duty to protect life. The ruling in *Lambert v. France* shows that withdrawing life-sustaining treatment does not violate the right to life when proper legal safeguards exist. However, laws vary across Europe and when reflecting on ongoing disagreements on end-of-life rights, societies must decide whether passive euthanasia is an exercise of the individual's autonomy or a potential risk to human rights, ensuring a balance between dignity and protection.

[20] Judgement of the ECtHR of June 13, 2024, *Lambert and Others v. France*, § 40.
[21] Judgement of the ECtHR of June 13, 2024, *Lambert and Others v. France*, § 80.
[22] Judgement of the ECtHR of June 13, 2024, *Lambert and Others v. France*, § 148.
[23] Judgement of the ECtHR of June 13, 2024, *Lambert and Others v. France*, § 151.
[24] Judgement of the ECtHR of June 13, 2024, *Lambert and Others v. France*, § 167.

3. Assisted Suicide

Assisted suicide is the act of intentionally providing a person with the means or knowledge to end their own life, typically through the prescription or supply of lethal substances, upon their voluntary and competent request. The final act leading to death is carried out by the individual, rather than a third party. The debate concerning assisted suicide is complex and usually highly emotional for both sides. The arguments for allowing this measure include that it protects patients autonomy and freedom of choice, relieves their suffering and allows families to be involved in the process, which may help alleviate their grief and lastly, that it preserves patients' dignity.[25]

The legal status of assisted suicide varies across the world, with some countries recognizing it as an individual right and others strictly prohibiting it. Currently, physician-assisted suicide can be legally practiced in the Netherlands, Belgium, Luxembourg, Colombia, and Canada. It is also legal in 5 US states and Switzerland.[26] Switzerland has an uncommon position on assisted suicide, as it is legally condoned and can be performed by non-physicians.[27]

The ECtHR approaches assisted suicide through the lens of personal autonomy and state obligations under the Convention. In cases like *Gross v. Switzerland* or *Pretty v. the United Kingdom* the ECtHR aims to find the balance between individual rights and the state's duty to protect vulnerable persons from abuse or undue pressure.

The ECtHR's ruling in *Pretty v. the United Kingdom* represents a significant moment in the legal debate surrounding the right to die. In this case, Mrs. Pretty suffered from terminal illness—a progressive neuro-degenerative disease of motor cells within the central nervous system. It is associated with progressive muscle weakness affecting the voluntary muscles of the body and causing severe weakness of the arms, legs and muscles involved in the control of breathing. Death is usually a result of muscle weakness, leading to respiratory failure and pneumonia.[28] There is no treatment that can prevent the progression of this disease. Diane Pretty wished to be able to control how and when she dies and thereby be spared suffering and indignity. Although it is not a crime to commit suicide under English law, she was prevented by her disease from taking such a step without someone else's assistance.

---

[25] L. Sue Baugh, "Assisted Suicide," *Encyclopedia Britannica*, https://www.britannica.com/topic/assisted-suicide, accessed 16 March 2025.

[26] Ezekiel J. Emanuel et al., "Attitudes and Practices of Euthanasia and Physician-Assisted Suicide in the United States, Canada, and Europe," *Jama* 316, no. 1 (2016): 86–87, https://doi.org/10.1001/jama.2016.8499.

[27] Samia A. Hurst and Alex Mauron, "Assisted Suicide and Euthanasia in Switzerland: Allowing a Role for Non-Physicians", *BMJ* 326, no. 7383 (2003): 271–73, https://doi.org/10.1136/bmj.326.7383.271.

[28] Judgement of the ECtHR of April 29, 2002, *Pretty v. the United Kingdom*, application no. 2346/02, § 7.

As a consequence, she sought the right to have her husband assist her in ending her life. It is however a crime to assist another to commit suicide.[29]

The applicant argued that the prohibition of assisted suicide violated her rights under the Convention. She submitted that permitting her to be assisted in committing suicide would not be in conflict with Article 2 of the Convention, as it protected the right to life and not life itself. She stated that the sentence concerning deprivation of life was directed towards protecting individuals from third parties, not from themselves. Article 2 of the Convention therefore acknowledges that it is for the individual to choose whether or not to go on living and reserves her right to die in order to avoid inevitable suffering and indignity.[30] Moreover, she argued that her right to autonomy under Article 8 (the right to respect for private life and family life) was violated by the prohibition of assisted suicide, as it prevented her from choosing the way she dies.[31]

Mrs. Pretty also stated that her suffering from a terminal disease amounted to degrading treatment under Article 3 of the Convention, which imposes both a negative obligation on the state to refrain from such treatment and a positive obligation to protect individuals from it. The applicant contended that this right was absolute and could not be balanced against community interests and that the blanket ban on assisted suicide violated Article 3 of the Convention by denying her protection from unbearable suffering without considering her specific circumstances.

However, the ECtHR ruled against her, stating that the right to life under Article 2 of the Convention does not extend the right to die. Article 2, which guarantees the right to life, imposes a positive obligation on states to protect life and this cannot be interpreted as a right to end one's life. The first sentence of this article enjoins the state not only to refrain from the intentional and unlawful taking of life, but also to take necessary steps in order to safeguard the lives of those within its jurisdiction.[32] The ECtHR found that UK's law on assisted suicide was a justifiable restriction under Article 8(2) of the Convention, and held that prohibition of assisted suicide served a legitimate aim of protecting vulnerable individuals from potential abuse and it was a necessary measure in a democratic society.[33]

Similarly, the ECtHR concluded that there is no positive obligation under Article 3 of the Convention to require the state to allow assisted suicide or to prevent the prosecution of the applicant's husband for helping her. While sympathetic to the applicant's situation, the ECtHR found that Article 3 of the Convention does not extend to sanctioning actions intended to end life and therefore, there was no violation of Article 3 of the Convention in this case.

---

[29] Judgement of the ECtHR of April 29, 2002, *Pretty v. the United Kingdom*, § 9.
[30] Judgement of the ECtHR of April 29, 2002, *Pretty v. the United Kingdom*, § 35.
[31] Judgement of the ECtHR of April 29, 2002, *Pretty v. the United Kingdom*, § 17.
[32] Judgement of the ECtHR of April 29, 2002, *Pretty v. the United Kingdom*, § 51.
[33] Judgement of the ECtHR of April 29, 2002, *Pretty v. the United Kingdom*, § 78.

In essence, the ruling reinforced the principle that while individuals may have rights to personal autonomy, they are to be balanced with States' interests in preserving life and protecting public order. The ruling in *Pretty v. United Kingdom* affirmed that the right to life under Article 2 does not extend to a right to die. Furthermore, it reinforced the principle that States have a legitimate interest in protecting vulnerable individuals. The case has had a lasting impact on end-of-life legal debates in Europe, influencing later the Convention rulings and national policies on euthanasia and assisted suicide. It highlighted the tension between personal autonomy and the state's duty to protect life, a debate that continues to shape discussions on assisted dying laws across Europe and beyond.

Issues raised in this case have seen differing viewpoints in other jurisdictions. For example, in the Canadian case of *Rodriguez v. British Columbia* Justice McLachlin dissented, emphasizing the importance of individual autonomy in end-of-life decisions. She stated that this is part of the persona and dignity of the human being that he or she has the autonomy to decide what is best for his or her body.[34] While the ECtHR did not feature dissenting opinions in *Pretty v. United Kingdom*, discussions in other courts, such as the Canadian Supreme Court, have also presented alternative viewpoints emphasizing individual autonomy in the context of assisted suicide.

Critics of the *Pretty v. United Kingdom* ruling argue that the decision placed state interests above individual autonomy, denying terminally ill patients the right to make deeply personal choices about their own bodies. They contended that Article 2 should not be interpreted as an obligation to live but rather as a protection against unjustified deprivation of life, meaning that individuals should have the right to refuse prolonged suffering. Furthermore, while the ECtHR acknowledged that Article 8 includes autonomy in medical decisions, it ultimately prioritized abstract concerns over the real and immediate suffering of the individual**.** This restrictive approach contrasts with evolving legal and ethical perspectives in countries like Canada and the Netherlands, where assisted dying is perceived as a part of patient's dignity and compassionate end-of-life care.

The ECtHR's ruling *Gross v. Switzerland* was another landmark decision on end-of-life care, affirming that a Swiss woman, Ms. Alda Gross, an elderly but not terminally ill individual, wished to end her life with medical assistance.[35] Swiss law permits assisted suicide under certain conditions, but doctors refused to prescribe her a lethal dose because she lacked a diagnosed terminal illness.[36] She argued that Switzerland's legal framework was unclear and prevented her from exercising her right to end her life in a dignified manner. The applicant claimed that Switzerland's

[34] Judgement of the Supreme Court of Canada of September 9, 1993, *Rodriguez v. British Columbia*, CanLII 75 3 SCR 519.

[35] Judgement of the ECtHR of September 30, 2024, *Gross v. Switzerland*, application no. 67810/10.

[36] Judgement of the ECtHR of September 30, 2024, *Gross v. Switzerland*, § 15.

refusal violated Article 8 of the Convention and argued that this includes the right to decide when and how to die.

The ECtHR ruled in favour of Ms. Gross, stating that Switzerland indeed lacked clear and foreseeable legal guidelines on assisted suicide, thus resulting in legal uncertainty. Moreover, Article 8 of the Convention was violated because the legal ambiguity prevented Ms. Gross from exercising personal autonomy over her own death.[37]

Although the *Gross v. Switzerland* ruling was ultimately nullified (before Switzerland could respond, it was revealed that Ms. Gross had already taken her own life, leading the ECtHR to dismiss the case), it remains significant in the broader debate on assisted suicide and legal clarity in end-of-life decisions. This case highlighted the growing recognition of personal autonomy under Article 8, suggesting that the right to private life includes the ability to decide when and how to die. It also underscored the need for clear and foreseeable legal guidelines on assisted suicide in order to prevent uncertainty. The case contributed to ongoing discussions in European human rights law about balancing state interests in protecting life with individual rights to end-of-life decisions, influencing later cases and policy discussions.

Summary

As follows from the above considerations, the European Court of Human Rights' case-law clearly indicates that the Convention provisions, including Article 2, Article 3, and Article 8, in particular, do not guarantee the right to death. Despite the lack of such a guarantee, the ECtHR does not prohibit national laws that legalize active and passive euthanasia, as well as assisted suicide. However, this is linked to the obligation of states to ensure appropriate safeguards protecting individuals who resort to any form of euthanasia and assisted suicide from abuses and violations of their rights guaranteed by the Convention. Issues related to the end of life thus remain within the wide margin of appreciation of Member States. This does not mean, however, that the ECtHR's rulings have not raised controversy: quite the opposite is true; as pointed out in this article, they have supporters and opponents, both advocating for either a complete ban on euthanasia or its full legalization. After all, it poses a challenge to apply the Convention provisions that at the same time and with equal legal force obligate Member States to protect human life and prohibit intentional killing while also protecting the right to privacy and individuals' choices concerning when and how to end their lives.[38]

[37] Judgement of the ECtHR of September 30, 2024, *Gross v. Switzerland*, § 35.

[38] Michał Balcerzak, "Euthanasia and Withdrawal of Life-Sustaining Treatment in the Case-Law of the European Court of Human Rights: Twenty Years After Pretty v. United Kingdom," *Prawo i Więź* 46, no. 3 (2023): 127–30, https://doi.org/10.36128/PRIW.VI46.699.

BIBLIOGRAPHY

Balcerzak, Michał. "Euthanasia and Withdrawal of Life-Sustaining Treatment in the Case-Law of the European Court of Human Rights: Twenty Years After Pretty v. United Kingdom." *Prawo i Więź* 46, no. 3 (2023): 115–132. https://doi.org/10.36128/PRIW.VI46.699.

Baugh, L. Sue. "Assisted Suicide." *Encyclopedia Britannica*. Accessed 16 March, 2025. https://www.britannica.com/topic/assisted-suicide.

Brassington, Iain. "What Passive Euthanasia Is." *BMC Medical Ethics* 21, no. 41 (2020): 1–13, https://doi.org/10.1186/s12910-020-00481-7.

Deliens, Luc, and Gerrit van der Wal. "The Euthanasia Law in Belgium and the Netherlands." *The Lancet* 362, no. 9391 (2003): 1239–40, https://doi.org/10.1016/S0140-6736(03)14520-5.

Emanuel, Ezekiel J., Bregje D. Onwuteaka-Philipsen, John W. Urwin, and Joachim Cohen. "Attitudes and Practices of Euthanasia and Physician-Assisted Suicide in the United States, Canada, and Europe." *Jama* 316, no. 1 (2016): 1. https://doi.org/10.1001/jama.2016.8499.

Garrard, Eve, Wilkinson, Stephen. "Passive Euthanasia." *Journal of Medical Ethics* 31, no. 1 (2024): 64–68. https://doi.org/10.1136/jme.2003.005777.

Gesang, Bernward. "Passive and Active Euthanasia: What Is the Difference?" *Medicine, Health Care and Philosophy* 11, no. 2 (2008): 175–80. https://doi.org/10.1007/s11019-007-9087-x.

Hurst, Samia A., and Alex Mauron. "Assisted Suicide and Euthanasia in Switzerland: Allowing a Role for Non-Physicians." *BMJ* 326, no. 7383 (2003): 271–73, https://doi.org/10.1136/bmj.326.7383.271.

Sandor, Judit. "A Lawyer's Legacy: The Significance of the Dániel Karsai v. Hungary Case." *Pravni Zapiši* 15, no. 3 (2024): 311–26.

Śliwka, Marcin, and Aneta Gałęska-Śliwka. "Regulating End-of-Life Decisions in Poland: Legal Dilemmas." *Advances in Palliative Medicine* 10, no. 2 (2021): 49–56. https://journals.viamedica.pl/advances_in_palliative_medicine/article/view/29332.

ZESZYT PRAWNICZY UAM
NR 15/2025
https://doi.org/10.14746/zpuam.2025.15.6

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

DOMINIKA PRZYDACZ

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0000-6379-5419
domprz5@st.amu.edu.pl

European Union Taxonomy—Can It Be an Effective Instrument for Legal Protection of Investors Against Greenwashing?

Abstract: The article addresses legal issues related to Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088. The regulation is analysed in the context of greenwashing with a view to determining whether it can be an effective legal protection instrument for investors in the financial products market. The provisions of the Regulation are analysed from a legal-dogmatic perspective, according to linguistic, functional and systemic interpretation, without skipping social and economic aspects. The text discusses greenwashing itself and its legal qualification under Polish and EU law. It also compares the legal situation of consumers and investors, focusing on the scope of legal protection that both groups could benefit from in the event of suffering damage.

Keywords: taxonomy, sustainable investments, greenwashing, stakeholders, financial market

Introduction

Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020[1] establishes a framework to facilitate sustainable investment. In its context, greenwashing should be considered first and foremost by referring to the formal circle of addressees of the Regulation—entities of the financial market.

However, it is also worth considering the informal addresses scope of the Regulation. As the taxonomic requirements are applied by financial institutions, some entities not covered by the Regulation, wishing to obtain financing for their investments, may also start to voluntarily apply the taxonomic classification.[2] This would involve obtaining financing on preferential terms, such as lower interest rates on loans. With this in mind, it is also possible to consider whether the attempt to reduce greenwashing has the potential to have an impact on a wider scale, beyond financial institutions.[3]

A broader perspective on the framing of this problem is important for two reasons. Firstly, it allows the legal protection of consumers and investors against

[1] Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088 (OJ L 198, 22.6.2020, pp. 13–43), hereinafter: the Regulation, Taxonomy or Taxonomy Regulation.

[2] Marleen Och, *The Taxonomy Regulation and the Prevention of Greenwashing* (Jean Monnet Centre of Excellence on Sustainable Finance and Law, 2024), 6.

[3] Och, *The Taxonomy Regulation and the Prevention of Greenwashing*, 6.

the effects of greenwashing to be contrasted. Thus, the legal protection instruments available to both groups can be compared. In addition, when analysing the situation of investors in the financial market, one cannot ignore the consumer protection acquis, which can also be drawn upon when shaping the legal situation of investors.

Secondly, the Taxonomy itself has the potential to have an impact on minimising the negative effects of greenwashing in industries other than just financial. For this reason, it is also necessary to consider the impact of the Taxonomy on improving the legal position not only of investors, but also of consumers. Although the Taxonomy imposes public disclosure obligations on financial market operators and Member States, other businesses wishing to demonstrate the sustainability of their operations can also act in accordance with its provisions.[4]

This article has been developed using the legal-dogmatic method, taking into account linguistic, functional and systemic interpretation, as well as socio-economic context. It is also important to verify whether the provisions of Taxonomy are likely to have an impact on the market and in what way, and therefore it is necessary to take the sociological impact of the law into account.

The conclusions of this study are relevant in view of the prevalence of greenwashing and the potentially existing loopholes in the legal system for investor protection from greenwashing in the financial market. The aim of the study is to broaden the legal perspective of the impact of greenwashing beyond consumers to investors and to add to the emerging literature on this subject.

Although there are some legal doubts as to the range of entities qualifying as consumers, also in the context of a possible extension of consumer protection to retail investors, the issue of such qualification is not the subject of this article. For the purposes of this analysis, based on the applicable legal provisions, the concept of a consumer and an individual investor as a client of a financial institution should be separated.

This paper describes the framework from the perspective of an investor using investing products, i.e. an individual investor who makes their own investment decisions based on the information provided to them by issuers. However, individual investors can use a number of different investment products, such as stocks, mutual funds or ETFs.

1. Greenwashing Phenomenon

Greenwashing is a marketing effort to create the perception in the minds of consumers that a product or service is green.[5] The actual environmental impact of the

[4] Och, *The Taxonomy Regulation and the Prevention of Greenwashing*, 7.

[5] Zuzanna Ochońska, "Ochrona konsumentów w branży mody," *Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej*, no. 3 (2021): 161.

product remains irrelevant, and the viewer only receives a message that they are dealing with a 'green', 'ecological' or 'environmentally sustainable' product.

Greenwashing can take the form of direct lying or misrepresentation in relation to the manufacturing process of a product or the materials from which it is made.[6] For example, the recipient may receive false information that the product is made from recycled materials or that the local ecosystem or its animals were not harmed during the production process.[7]

In the context of the financial market, misleading information may refer to the untruthful composition of an investment portfolio or an investment fund that does not fund sustainable investments at all. In the context of the Regulation, information on an organisation's human and labour rights compliance practices and corporate governance is also relevant. Therefore, transparency of information provided to investors is to be multi-faceted and sustainable.

Greenwashing mainly refers to environmental misstatements, but in this context, it is increasingly a matter of falsification of corporate governance and social factors (also called bluewashing). If companies fail to comply with financial law or prevent money laundering, they will also be fined for greenwashing.[8]

Greenwashing has grown in popularity as the demand for environmentally sustainable products has increased. This was primarily influenced by the tendency of consumers to pay more attention to important non-financial values.[9] Consumers began to pay attention to products in line with respect for the environment and human rights.[10]

Green investments have also gained in importance, and investors are more likely to direct their capital into profitable as well as sustainable ventures. Capital from sustainable financial instruments already represents an incalculable value on the capital markets in Poland and worldwide, and investors are also showing interest in instruments with a low climate risk that provide sustainable, long-term returns.[11] An investment strategy based on long-term investment in sustainable financial instruments appears to investors as low-risk. However, a prerequisite for such an investment to yield a stable return is the reliability of the information provided with regard to sustainability.

---

[6] Ochońska, "Ochrona konsumentów w branży mody," 161.

[7] Célia Santos et al., "A Systematic Literature Review on Greenwashing and Its Relationship to Stakeholders: State of Art and Future Research Agenda," *Management Review Quarterly* 74, 2024: 1398, https://doi.org/10.1007/s11301-023-00337-5.

[8] "Deutsche Bank-Owned Asset Manager DWS Fined $27 Million for Greenwashing," Reuters, published 2 April 2025, https://www.reuters.com/sustainability/german-asset-manager-dws-fined-25-mln-eur-greenwashing-case-2025-04-02/.

[9] Santos et al., "A Systematic Literature Review on Greenwashing and Its Relationship to Stakeholders," 1398.

[10] Magdalena Mikołajek-Gocejna, *Europejski rynek inwestycji społecznie odpowiedzialnych: perspektywa rynku kapitałowego* (Oficyna Wydawnicza SGH, 2021), 11.

[11] Katarzyna Szwarc and Stanisław Stefaniak, *Klimatyczne wyzwania na rynku finansowym w Polsce* (Instrat Foundation, 2020), 63.

2. Negative Effects of Greenwashing

The biggest risk to the consumer from greenwashing is that he or she will be misled and support unreliable traders. For the consumer, therefore, it is primarily moral damage. However, greenwashing can also be considered through the prism of adverse disposal of consumer resources. A disproportionately high price usually has to be paid for falsely green products and consumers are statistically willing to accept a higher price in return for the product being in line with their world view.[12] However, receiving an unethical product, at an inflated price, can be seen as damage to the consumer's property.

However, the immediacy of this harm is minimised due to the fact that the consumer is the final recipient of the product in the supply chain. Nonetheless, consumers are given special protection in the market: the legislation ensures that they are protected from greenwashing and can seek redress if they suffer damage .In the case of investment in a negatively impacting activity, this harm already direct impacts the investor and the capital that could have been invested in a socially responsible activity. Investing capital in a product that is not environmentally responsible has an impact on the exploitation of the environment and human resources, potentially at all stages of the value chain. Furthermore, the relationship of the investor with the financial institution is more direct than that of the consumer with the entrepreneur. Investors also bear the risk associated with changes in capital market trends, which, in the case of climate risk, can change dynamically. The fact that greenwashing is disclosed may also initiate a downward trend in the instrument concerned.[13]

The risks posed by greenwashing are therefore multifaceted. Greenwashing threatens the interests of consumers and investors and violates the principles of fair competition in the market.[14] In the case of investment activities, which are themselves associated with risk taking, it appears to be an additional nuisance and a brake on the promotion of environmentally sustainable investments. In the context of EU climate policy, it should also be emphasised that greenwashing can have a negative impact on financing the green transition. Indeed, greenwashing provides a source of financing for investments based on low-carbon and environmentally friendly technologies. However, investor awareness of greenwashing practices may create an aversion towards green financial instruments and cause investors to abandon investing in this sector altogether.

Greenwashing is therefore unequivocally negative for the market and should be combated both through education and awareness-raising for all market participants,

[12] Mark Segal, "Consumers Willing to Pay 12% Premium for Sustainable Products: Bain Survey," ESG Today, published 14 November 2023, https://www.esgtoday.com/consumers-willing-to-pay-12-premium-for-sustainable-products-bain-survey/.

[13] Santos et al., "A systematic Literature Review on Greenwashing and Its Relationship to Stakeholders," 1398.

[14] Santos et al., "A Systematic Literature Review on Greenwashing and Its Relationship to Stakeholders," 1410.

but also by providing appropriate legal protection instruments. As greenwashing causes damage to both the environment and individuals, they should be able to seek redress under existing law.

3. Legal Context of Greenwashing

The problem of greenwashing has so far been most strongly regulated in competition and consumer protection law. This is due to the need to extend special legal protection to consumers to counterbalance their unequal position *vis-à-vis* companies. However, in the financial market, this problem has not yet been particularly recognised and nor have investors themselves been covered by such protection, with the legal position of investors *vis-à-vis* issuers also remaining unequal.

Moreover, for the investor, the only source of knowledge about a particular financial instrument is often the issuer itself, which can shape this information in any way it wishes. The supply chain for consumer products usually involves more actors, which also increases the chance of the consumer being able to independently verify information about the alleged environmental performance of a product. All it takes is for one of the actors in the supply chain to appear to be an unreliable supplier, which can already lead the consumer to suspect greenwashing.

It is only with the development of the concept of sustainable finance that attention has turned to ensuring that sustainability information provided to investors is transparent and subject to scrutiny by regulators. The regulation of sustainability disclosure in the Taxonomy is intended to serve this purpose. The Regulation is therefore an attempt to fill this regulatory gap and represents an important step towards extending legal protection to investors. This deserves attention especially in view of the fact that consumers enjoy relatively broad protection.

The fight against greenwashing on the Polish financial market is dealt with by the Komisja Nadzoru Finansowego (KNF, Financial Supervision Commission). It is therefore possible to distinguish at least two public authorities in Poland that deal with combating greenwashing—the Financial Supervision Commission and the Urząd Ochrony Konkurencji i Konsumentów (UOKiK, Office for the protection of Competition and Consumers).

However, it should be emphasised that there are few bodies in Poland dedicated to combating greenwashing, and for both the KNF and the UOKiK, this is only a minor part of their activities. The nature of actions taken by these authorities to combat greenwashing varies. Most investigations are undertaken by the UOKiK *ex officio*.[15] Victims can notify the Office of a trader's unfair practices, although the

[15] "Komunikat w sprawie działalności UOKiK w 2022 roku," UOKiK Archive, published 7 March 2023, https://archiwum.uokik.gov.pl/aktualnosci.php?news_id=19396.

percentage of cases initiated on the basis of a notification is significantly lower. This confirms the active role of the UOKiK in identifying and combating greenwashing on the consumer market.

Unlike the UOKiK, the KNF initiates its proceedings primarily on the basis of notifications coming from interested parties. Due to the fact that the KNF's actions are, as a rule, covered by professional confidentiality, in the case of a notification of irregularities, the notifying person will not receive a response to the information he or she has sent, nor will he or she receive a communication on how the commission uses the information. The proceedings are therefore less transparent than in the case of consumers. This has a negative impact on identifying possible damages and claims by investors.

There is also an arbitration court within the KNF that supports the resolution of disputes in the financial market. The KNF additionally supports consumers with its activities, for example, by providing Banking Consumer Arbitration services. An aggrieved person can also obtain free legal assistance from the Financial Ombudsman. Thus, within the framework of financial supervision, the KNF ensures that consumers can pursue their claims. However, the above-mentioned institutions are not directed at the legal protection of investors in the financial market.

Nevertheless, KNF independently monitors and detects manipulation or greenwashing. The KNF undertakes appropriate verification activities, such as requesting additional explanations or providing evidence supporting the disclosures in the reports,[16] and in case of a crime being suspected, it may file a notice to law enforcement organs. The KNF also stresses the importance of including climate risks in financial reports.[17] Supervisors can verify issuers disclosed commitments to climate targets to prevent the occurrence of greenwashing.

Under EU law, consumers are comprehensively protected from greenwashing. The most important EU document shaping the legal situation for consumers is the new 2020 Consumer Agenda. The programme identifies five key areas of the internal market that require action, including green transformation, redressability and enforcement of consumer rights.[18] It is pointed out that providing consumers with better protection against greenwashing and premature obsolescence of products will strengthen their role in the process of developing a sustainable economy.[19] However, it should be noted that the role of investors in the green transition is equally important, however, this is not enough to provide similar protection to this group.

[16] "Europejskie wspólne priorytety nadzorcze w odniesieniu do rocznych raportów finansowych za rok 2022," Komisja Nadzoru Finansowego, last modified 17 October 2025, https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/dokumentyESMA.

[17] "Europejskie wspólne priorytety nadzorcze w odniesieniu do rocznych raportów finansowych za rok 2022."

[18] Communication from the Commission to the European Parliament and the Council, "New Consumer Agenda Strenghtening Consumer Resilience for Sustainable Recovery," Brussels, 2020, 1.

[19] "New Consumer Agenda Strenghtening Consumer Resilience for Sustainable Recovery," 12.

Consumers are protected by such legal measures as the Directive on unfair business-to-consumer commercial practices. EU rules provide consumers with a right to proportionate and effective remedies, in particular, to compensation or a price reduction or the possibility to terminate the contract with the trader.[20] They therefore provide the basis for claiming liability for damages for greenwashing practices.

Greenwashing in Poland is considered unlawful under the Act on Combating Unfair Competition, as an act of unfair competition.[21] Indeed, greenwashing consists of disseminating false or misleading news about one's business for the purpose of gaining an advantage, which fulfils the statutory definition of this tort.[22] Importantly, businesses are not required to provide information that is completely false about the environmental aspects of their business for their action to be deemed unlawful. It is sufficient for it to be partially incomplete, untrue, manipulated or made available in such a way as to be intentionally misleading. The information made available by traders may relate to the persons in charge of the enterprise, the products or services manufactured, the prices charged, or the economic or legal situation.[23]

Particularly relevant in the environmental context is the fact that the use of false attestations, unreliable test results or information on distinctions or labels for products or services, also fulfils the elements of a tort.[24] Thus, within the consumer market, the legal qualification of greenwashing is unambiguous and such practices are considered incompatible with EU and Polish law. The Taxonomy, by setting out obligations to ensure transparency in product certification and labelling, also attempts to combat greenwashing. It extends its scope to the financial market, filling a hitherto existing gap in the law.

Although greenwashing practices undertaken on the consumer and financial markets are, in essence, no different, investors cannot expect protection similar to that of consumers, and financial supervisory institutions in Poland do not specialise in combating greenwashing. The disproportion regarding the regulation of greenwashing is therefore apparent, even taking into account the different nature of the activities undertaken by investors and consumers.

The main manifestation of greenwashing of financial instruments in the Taxonomy's concept—the use of inconsistent, misleading labels and certificates intended to confirm the environmental performance of products—if it referred to consumers, would also be qualified as a prohibited act under Polish legislation.

---

[20] "Nieuczciwe praktyki handlowe," Your Europe, https://europa.eu/youreurope/citizens/consumers/unfair treatment/unfair-commercial-practices/index_pl.htm, accessed 27 March 2025.

[21] Ochońska, "Ochrona konsumentów w branży mody," 162.

[22] Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (consolidated text Journal of Laws of 2022, item 1233 as amended).

[23] Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (consolidated text Journal of Laws of 2022, item 1233 as amended).

[24] Igor B. Nestoruk, "Marketing ekologiczny w prawie polskim—przegląd regulacji," *Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej*, no. 3 (2011): 156.

Therefore, it is worth emphasizing the relevance of the Taxonomy regulation, in the context of addressing this problem. The overarching goal of the Regulation is to eliminate situations in which an entrepreneur would use false data. Restricting similar practices would be valuable not only for the investors themselves, but also for the green transition process, by increasing capital flows to sustainable investments.

4. Legal Qualification of Greenwashing Under the Provisions of the Taxonomy

The standards regulated by the Regulation are of a public law nature. While it is businesses that are required to implement and adhere to the classification of the Taxonomy, member states and the EU itself are addressees of certain provisions of the Regulation.[25] The competent authorities of the states and the EU use the Taxonomy system to determine whether a business qualifies as environmentally sustainable, in any new labelling schemes for financial products or corporate bonds labelled as sustainable.

Competent authorities should therefore apply their authority to all measures regarding the systematics of sustainable activities. When creating any new designation of a product or service as environmentally sustainable, EU and EU countries must create it in accordance with the taxonomy classification. The obligation of member states to use uniform indicators of environmentally sustainable activities is an expression of strong regulatory harmonization and is intended to prevent fragmentation of rules operating within the internal market.[26] However, not all member states agree with the taxonomy classification, which has even led to judicial conflicts at the EU level.[27] The conflicts mainly concern the recognition of gas and atom as sustainable energy sources.[28]

Fragmentation of regulations in this area, potentially progressing in the future, could lead to damage to investors' interests. Differentiating the systematics of sustainable activities, would significantly hinder the undertaking of environmentally friendly investments.[29] It would also translate into an insufficiently transparent information policy towards investors. It would also be easier to mislead investors or manipulate certain non-financial information.

---

[25] Och, *The Taxonomy Regulation and the Prevention of Greenwashing*, 3.

[26] Radosław Maruszkin et al., *Taksonomia: komentarz do rozporządzenia 2020/852 w sprawie ustanowienia ram ułatwiających zrównoważone inwestycje* (C.H. Beck, 2022), 34.

[27] Action brought on 7 October 2022—*Austria v. Commission* (Case T-625/22) (OJ C 24, 23.1.2023, pp. 43–45).

[28] Rafał Bujalski, *UE będzie wspierać inwestycje w atom i gaz* (LEX/el., 2022).

[29] Och, *The Taxonomy Regulation and the Prevention of Greenwashing*, 3.

Entrusting competent state authorities, under the provisions of the Regulation, with the supervision of information obligations of entrepreneurs is a way to increase investor awareness and legal protection, while at the same time securing financing for the green transition from private sector funds. Supervisors have the duty to verify and control the information provided to investors by issuers.

Greenwashing, as a problem requiring public regulation, is addressed in Article 4 of the Regulation. While standards for transparency of pre-contractual information made available by businesses and in periodic reports are regulated in other provisions of the Regulation, Article 4 sets out the competence of Member States and the EU to create a taxonomy-based qualification of business activities as environmentally sustainable.

This is a key instrument needed to ensure uniform regulations aimed at qualifying and reducing greenwashing in the financial market sector. The commitment of countries to a uniform classification system is intended to allow investors to safely undertake sustainable investments while minimizing the risk of greenwashing.[30] In addition, ensuring public oversight of the information made available to investors in progress reports and before entering into a contract with an investor can be an effective way to control greenwashing.

Requiring member states to transpose the taxonomy's systematics into national labelling or certification systems significantly reduces the risk of entrepreneurs using unreliable green credentials. An important question, however, remains how broad the scope of information disclosed by entrepreneurs will be, and whether it will actually coincide with the requirements of the Taxonomy.

Additionally, the ability to verify the authenticity of information presented to investors may prove to be problematic. This is likely to be the most important function of regulators and auditors, given that investors have limited ability to confirm all information presented to them. Investors may also find it difficult to verify information, especially if sustainability reports do not reference the necessary source documents.[31] Auditors will continue to attest ESG reports under the rigor of limited liability for another two years. National sustainability attestation standards are being created for the first time and will probably be refined over time, with the auditors likely taking their first attestation applications in 2025.[32]

In the event of possible non-compliance with the Taxonomy, financial market regulators are also competent to impose sanctions on traders. However, as a result of the above, supervisors and auditors themselves first need to learn how to practically confirm the information provided by traders in order to be able to effectively apply

[30] Maruszkin et al., *Taksonomia*, 35.

[31] Och, *The Taxonomy Regulation and the Prevention of Greenwashing*, 12.

[32] Ustawa z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym (consolidated text Journal of Laws of 2024, item 1035 as amended).

sanctions for violations, in particular, regarding the disclosure of information that is only partially true or manipulated, qualifying as greenwashing.

Thus, the above comments reveal a certain weakness of the Regulation's provisions. The issues of creating a unified systematics and paying attention to the issue of legal protection of investors in the financial market, were comprehensively addressed in the Taxonomy. However, despite the fact that member states and businesses have been obliged to comply with specific standards, supervisors and auditors may not be equipped at the outset with adequate tools to verify information relating to sustainability.

The preamble, as well as the legal provisions of the Regulation, indicate that greenwashing is the most important problem addressed by the Taxonomy.[33] However, this does not change the fact that simply designating public oversight of the information in question may not be sufficient to address it. Consequently, the actual level of investor protection against greenwashing across EU member states, may vary.

5. Issuers' Liability for Damages in the Context of Greenwashing

It is also important to consider the position of investors in light of the provisions of the Regulation itself. By designating public-law obligations, the Taxonomy also shapes the relationship between investors and entrepreneurs, thus penetrating the realm of private law. The provisions of the Regulation directly affect what information will go to investors and what quality that information will be.

Investor protection under the Regulation is based on the assumption that the Taxonomy will be uniform for the entire internal market. The Regulation also sets identical standards of protection for all member states, imposing the same obligations on supervisory authorities. However, it should not be overlooked that in each country the supervisory authorities may shape their policies differently. In particular, the authorities' powers or the level of education and awareness of individual investors may differ. It is therefore possible that the Taxonomy will prove insufficient for some countries to provide investors with adequate protection. An adequate level of investor protection can only be ensured in countries with a developed financial market.

Ultimately, a country's legal system is shaped in such a way that the law is as convenient as possible for the interests of the party currently in power.[34] Importantly, it is most often in the interests of the political parties in power to make relatively uncontroversial decisions and changes, which can make the implementation of

[33] Och, *The Taxonomy Regulation and the Prevention of Greenwashing*, 1.

[34] Zygmunt Ziembiński, *Problemy podstawowe prawoznawstwa* (Państwowe Wydawnictwo Naukowe, 1980), 23.

Taxonomy and ESG-related legislation more difficult. We already witnessed the first wave of withdrawal from sustainability reporting this year, with the proposals included by the European Commission in the Omnibus I package.[35]

It is also necessary to consider whether investors have the possibility of pursuing their claims on the basis of issuers' liability for damages at all. This is because there is no doubt that an investor acting under the influence of greenwashing and failing to receive adequate information about a financial instrument may suffer damages. If an investor decides to invest in environmentally sustainable instruments and the issuer fails to fulfil its obligations, this will constitute a violation of the Regulation.

It would seem, therefore, that in addition to sanctions from supervisory authorities, issuers could be liable under Articles 415 et seq. of the Polish Civil Code. However, in practice, demonstrating an adequate causal link between the violation of disclosure obligations and the investor's damage could be a significant impediment to pursuing claims.[36] This is because an investor would have to show that if the issuer had properly performed its disclosure obligations, the investor would not have made a risky investment decision. However, information relating to sustainability is general information and does not bear the hallmarks of a recommendation to a specific investor. Therefore, as a rule, such information should not be the primary and decisive factor in making a particular investment.

As mentioned earlier, it can be difficult for individual investors to verify the information presented by issuers. Investors often show too much trust in intermediaries, thereby failing to assess the risks associated with certain financial instruments.[37] For this reason, the vast amount of information pertaining to sustainability can constitute an additional factor creating uncertainty for the investor and may result in a hasty or risky investment decision. Under such conditions, investors may be particularly susceptible to greenwashing.

Consideration should also be given to whether investors could benefit from the protection against market manipulation provided by EU law.[38] Although the Market Abuse Regulation sets out a list of circumstances that may constitute manipulation, though not an exhaustive one, it is difficult to find greenwashing-re-

[35] Proposal for a Directive of the European Parliament and of the Council amending Directives (EU) 2022/2464 and (EU) 2024/1760 as regards the dates from which Member States are to apply certain corporate sustainability reporting and due diligence requirements, Brussels, 26.2.2025, COM/2025/80 final.

[36] Tomasz Sójka et al., *Cywilnoprawna ochrona inwestorów korzystających z usług maklerskich na rynku kapitałowym* (Wolters Kluwer Polska, 2016), 99.

[37] Tomasz Sójka et al., *Cywilnoprawna ochrona inwestorów korzystających z usług maklerskich na rynku kapitałowym*, 99.

[38] Regulation (EU) 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (OJ L 173, 12.6.2014, pp. 1–61).

lated phenomena there. Indeed, protection is provided against manipulation that is strictly related to the trading of financial instruments or the dissemination of information that is intended to facilitate the manipulation of asset prices. Greenwashing, on the other hand, should be considered more broadly, since a strategy based on it may also have long-term objectives, rather than short-term price fluctuations or share buybacks.

A distinction must also be made here between an investor using a brokerage service and one merely purchasing investment products. Although it is common to use brokerage services, not every investor wants to do so or trusts them. Even though an investor may use brokerage services, it is still the issuer that is held accountable for its legal obligations on delivering information to investors. The issue of the unreliability or unverifiability of data published as a part of the taxonomy reporting is not a matter of brokerage services, but issuer liability.

Not every investor will decide on brokerage services; after all, these also do not give full assurance of the success of the investment and do not fully reduce the investment risk. The financial market is only to a certain extent guided by technical analyses or trends, but is also driven by emotions, both of the investors themselves and the whole public mood caused by the current socio-economic context and unexpected events, including armed conflicts, impulsive political decisions, or volatile behaviour from the commodities market or currencies.

Investors may be particularly susceptible to aggressive marketing policies pursued by issuers of financial instruments. The practice of supervisory inspections will also assess whether the information provided by traders will be truly verifiable and objective. Indeed, entrepreneurs may engage in mere formalistic compliance with sustainability reporting, or may be more eager to incur financial sanctions than to comprehensively prepare such reports.

Disclosure obligations are intended as an instrument to protect investors in an unequal relationship with the issuer. It is also the only form of legal protection provided to investors under the Regulation. The entrepreneur's communications should be shaped in such a way as to prevent the exploitation of the unequal position in the market of these entities through the use of unethical promotional activities[39] such as greenwashing. Under the provisions of the Regulation, such protection is provided to investors both at the pre-contractual stage and at the time when the issuer is already providing brokerage services to the investor. In contrast, the possibility of asserting investor claims on the grounds of issuer liability for damages, in practice, may be extremely difficult or impossible to achieve.

[39] Tomasz Sójka et al., *Cywilnoprawna ochrona inwestorów korzystających z usług maklerskich na rynku kapitałowym*, 106.

Summary

In conclusion, it should be said that information obligations may have only limited effectiveness in protecting individual investors. Among the abundance of information about financial instruments, non-professional investors may not be able to select information that is key to assessing the risk of a particular investment. At the same time, however, the risks faced by investors are higher than those faced by consumers.

Investor protection in the financial market is therefore limited in nature and effectiveness. Although the provisions of the Taxonomy provide a certain standard of investor protection under disclosure obligations, they may be insufficient for effective enforcement of investors' claims. Also noteworthy is the disparity in the legal protection of investors and consumers from the risks arising from greenwashing. Comparing the potential losses and risks taken, the scope of protection and redress mechanisms is clearly disproportionate for both groups.

However, financial market regulators possess the tools to enforce greenwashing, and the fines imposed on companies for such practices are increasing. It is not only the taxonomic disclosures that are subject to supervisory review, but also the indicated risks and climate targets. Investors also have other legal mechanisms for their protection besides the corporate social responsibility or taxonomic regulations. Yet a more serious approach to sustainability at the EU and national level is a trend that is conducive to building broader legal protection for investors in the financial market against greenwashing and manipulation.

BIBLIOGRAPHY

Bujalski, Rafał. *UE będzie wspierać inwestycje w atom i gaz*. LEX/el., 2022.

Dampere, Juan, Ebrahim Alamash, and Paulo Mattos. "Uneiliving the Truth: Greenwashing in Sustainable Finance." *Frontiers in Sustainability* 5 (2024): 1362051. https://doi.org/10.3389/frsus.2024.1362051.

Maruszkin, Radosław, Jakub Bednarek, Magda Biernat-Kopczyńska, Tomasz Lasecki, and Tomasz Tamecki. *Taksonomia: komentarz do rozporządzenia 2020/852 w sprawie ustanowienia ram ułatwiających zrównoważone inwestycje*. Wydawnictwo C.H. Beck, 2022.

Mikołajek-Gocejna, Magdalena. *Europejski rynek inwestycji społecznie odpowiedzialnych: perspektywa rynku kapitałowego*. Oficyna Wydawnicza SGH, 2021.

Nestoruk, Igor B. „Marketing ekologiczny w prawie polskim—przegląd regulacji." *Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej*, no. 3 (2011): 143–67.

Och, Marleen. *The Taxonomy Regulation and the Prevention of Greenwashing*. Jean Monnet Centre of Excellence on Sustainable Finance and Law, 2024.

Ochońska, Zuzanna. „Ochrona konsumentów w branży mody." *Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej*, no. 3 (2021): 148–62.

Santos, Célia, Arnaldo Coelho, and Alzira Marques. "A Systematic Literature Review on Greenwashing and Its Relationship to Stakeholders: State of Art and Future Research Agenda." *Management Review Quarterly* 74, 2024: 1398–421. https://doi.org/10.1007/s11301-023-00337-5.

Sójka, Tomasz, Katarzyna Klafkowska-Waśniowska, Maciej Mataczyński, and Rafał Sikorski. *Cywilnoprawna ochrona inwestorów korzystających z usług maklerskich na rynku kapitałowym*. Wolters Kluwer Polska, 2016.

Szwarc, Katarzyna, and Stanisław Stefaniak. *Klimatyczne wyzwania na rynku finansowym w Polsce*. Instrat Foundation, 2020.

Ziembiński, Zygmunt. *Problemy podstawowe prawoznawstwa.* Państwowe Wydawnictwo Naukowe, 1980.

ZESZYT PRAWNICZY UAM
NR 15/2025
https://doi.org/10.14746/zpuam.2025.15.7

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

VANESSA MARIA ROSITO

University of Bari Aldo Moro, Italy
https://orcid.org/0009-0009-7033-515X
vanessa.rosito@uniba.it

Generational Change in Agriculture: Recent Italian Legislative Developments within the Framework of European Policies

Abstract: The lack of generational renewal and demographic aging represent crucial challenges for European agriculture. The CAP 2023–2027 acknowledges the central role of young farmers in developing a competitive and sustainable agri-food system. In this context, Italian Law No. 36/2024 aims to promote youth entrepreneurship in agriculture through an integrated approach designed to facilitate young people's access to and permanence in the sector. This paper analyses the main issues related to generational change at both European and national levels, highlighting the need for greater policy integration. It then examines the most recent Italian regulatory approach, assessing its effectiveness in relation to the national entrepreneurial structure and the objectives of the European Union.

Keywords: young farmers, generational change, protection of rural areas, land access, pre-emption

Introduction

The demographic aging of the agricultural population and the insufficient generational turnover represent some of the most pressing challenges currently faced by European agriculture. These phenomena not only undermine the continuity and competitiveness of the sector, but also contribute to the socio-economic decline of rural areas, marked by depopulation, land abandonment, and reduced innovation. In this context, young farmers are increasingly seen as key actors in promoting a more sustainable, resilient, and innovative agri-food system.

Acknowledging this, the European Union has placed generational renewal among the strategic objectives of the Common Agricultural Policy (CAP) 2023–2027, encouraging Member States to adopt tailored measures aimed at attracting and supporting young people in agriculture. Against this backdrop, Italy has recently introduced Law No. 36/2024, a legislative intervention specifically designed to promote youth entrepreneurship in the agricultural sector. Through a multidimensional and integrated approach, this law seeks to overcome structural barriers to entry and permanence for young farmers by enhancing access to land, credit, training, and market opportunities.

1. The Reasons for Legislative Intervention to Promote and Develop Youth Entrepreneurship in Agriculture

On March 26, 2024, Law No. 36 of March 15, 2024, entitled "Disposizioni per la promozione e lo sviluppo dell'imprenditoria giovanile nel settore agricolo" (Provisions for the Promotion and Development of Youth Entrepreneurship in the Agricultural Sector) was published.

This legislative text follows the trend observed at European, national, and regional levels aimed at encouraging young people to enter the agricultural sector by identifying appropriate legal instruments to ensure the preservation of agricultural productive activities, guaranteeing their competitiveness and continuity.

The lack of generational turnover and demographic aging are some of the main issues affecting the European agricultural sector. The problem related to the age of agricultural entrepreneurs, predominantly male and over forty years old, significantly impacts the mortality of European agricultural enterprises. This trend affects rural areas, which are undergoing progressive depopulation and are increasingly utilised for non-agricultural uses, with negative repercussions in terms of biodiversity conservation and food security, making the European Union increasingly dependent on agricultural imports from non-EU markets.

The examination of the regulations introduced by Law no. 36/2024 cannot disregard the context emerging from statistical data, which shows European agriculture where family-run enterprises represent the vast majority of agricultural businesses in the European Union, accounting for 93% of the total, and only 6.5% of those have heads of enterprises with an age under thirty-five years of age.

Additionally, the data analysis reveals the uneven distribution of land. Four percent of all farms, those with more than 100 hectares, own about 52% of agricultural land; small farms, with less than 5 hectares, represent 40% of all farms and use only 6% of all available agricultural land.[1]

This strong concentration of land is a sign of the industrialization of agriculture, where a few large enterprises, focused on intensive production, can produce crops on a large scale and sell them globally.

This trend for agricultural concentration, facilitated by the current market structure and the model of direct payment distribution,[2] has a negative impact on the sustainability and resilience of agriculture, particularly in terms of vitality, employment, and enhancement of rural areas, as well as the protection of the environment, biodiversity, and landscape. The consequence is the abandonment of the agricultural

[1] Eurostat, Statistical Books, Agriculture, forestry and fishery statistics—2020 edition, cap. 2 Agriculture—the factors of production, available on the site: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Farms_and_farmland_in_the_European_Union_-_statistics&action=statexp-seat&lang=it.

[2] Pamela Lattanzi, "Le dimensioni aziendali nelle scelte della nuova Pac: le piccole aziende agricole," *Rivista di diritto agrario*, no. 2 (2022): 180.

sector by small enterprises, which are unable to establish themselves economically in the market, with negative implications for the vitality of entrepreneurship and rural areas.[3]

In Italy,[4] as with the European scenario, the agriculture sector is characterised by the progressive exit of small, family-run farms—often unable to sustain their activities—from the market and the growing detachment between land ownership and agricultural management due to increasing uncertainties about the future sustainability of agricultural activities. This leads to a tangible risk of abandoning agricultural productive activities, seen as one of the main obstacles to the competitiveness of the sector, with effects on the socio-economic vitality of rural areas in terms of depopulation, population ageing, and lack of innovation.[5]

In this context, the presence of young farmers would represent an opportunity to develop a competitive and sustainable food system in its economic, social, and environmental dimensions. However, numerous factors still hinder young people's access to agriculture. Specifically, as highlighted in the Commission's analysis, these factors are: economic factors, such as difficulties in accessing land due to high land prices, difficulties in accessing financial resources, market risks, and lack of infrastructure; cultural and social factors, represented by the perception of agricultural activity as an unattractive occupation unable to offer adequate social protection, and the difficult access to knowledge and innovations.[6]

Additionally, the low profitability of agricultural enterprises,[7] especially those that are individually owned and not part of aggregative organisations, discourages young people—who are increasingly often equipped with specialised degrees—from approaching agricultural activities.[8]

The objective of attracting young farmers to rural areas must be considered from a broader perspective, and the policy for generational turnover must be an integral part of a general agricultural policy direction. Recognising that agricultural

[3] Research for AGRI Committee: "The Future of the European Farming Model. Socio-economic and territorial implications of the decline in the number of farms and farmers in the EU," Policy Department for Structural and Cohesion Policies Directorate-General for Internal Policies, April 2022.

[4] Istat (2022). 7° Censimento generale dell'Agricoltura, https://7censimentoagricoltura.it/.

[5] https://www.pianetapsr.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/2866. See also "Giovani e Agricoltura. Rapporto 2024," Document created within the framework of "Programma Rete Rurale Nazionale 2014–22, Marzo 2024."

[6] Silvia Bolognini, "La comunicazione della Commissione europea "Il futuro dell'alimentazione e dell'agricoltura," *Rivista di diritto agrario*, no. 1 (2018): 110.

[7] Irene Canfora, "Raggiungere un equilibrio nella filiera agroalimentare. Strumenti di governo del mercato e regole contrattuali," in *Cibo e diritto. Una prospettiva comparata: Volume 1*, ed. Lucia Scaffardi and Vincenzo Zeno-Zencovich (Roma TrE-Press, 2020), 237; Laura Costantino, "La problematica dei prezzi dei prodotti agricoli: strumenti normativi tra antichi problemi e nuove crisi," *Rivista di diritto agrario*, no. 2 (2020): 783.

[8] With regard to the subjective category of young farmers, their weakness is underlined in "Whereas" 81 of Regulation (EU) no. 2021/2115, of the European Parliament and of the Council of 2 December 2021.

enterprises provide societal benefits by generating positive externalities,[9] efforts to attract young farmers to rural areas must include legal instruments, in addition to incentive measures, to ensure their entry and retention in the sector.

In this framework, on the one hand, EU policy develops and globally addresses the challenges posed by the agri-food chain considered as a whole, pursuing objectives aimed at creating a competitive and sustainable agri-food system.[10] On the other hand, Member States are in the best position to ensure the entry and retention of young people in agriculture.

While the new CAP implementation model entails greater responsibility for Member States, which must intervene at the national regulatory level to promote young people's access to agriculture, it also offers the possibility for individual Member States to structure strategies that are tailored to the domestic context, capable of reflecting the specific needs of young farmers.[11]

Accordingly, a brief overview of the principal tools supporting young farmers under the CAP and at the national level is necessary before delving into the innovations introduced by Law No. 36/2024.

2. Young Farmers in Light of the Common Agricultural Policy 2023/2027 and the National Strategic Plan

Generational change has always been considered a priority on the political agenda of the European Union. Over the years, the European legislator has provided significant support measures for young farmers in the awareness that these measures renew the entrepreneurial fabric of the sector, reduce the phenomenon of depopulation[12] by ensuring the permanence of families in rural areas and facilitating the inclusion of new productive forces.

The current Common Agricultural Policy 2023–2027 also continues to provide specific measures to support young farmers, recognising their important role in

[9] Franco Sotte et al., "Giovani e impresa in agricoltura," *Agriregionieuropa* 1, no. 2 (2005); Anna Carbone et al., "La misura giovani tra nuovo Regolamento sullo sviluppo rurale e prime evidenze dell'applicazione 2000–2003," *Agriregionieuropa* 1, no. 2 (2005).

[10] European Commission, "Strategic Dialogue on the Future of EU Agriculture. A Shared Perspective on Agriculture and Food in Europe (Final report)," 2024, https://agriculture.ec.europa.eu/document/download/171329ff-0f50-4fa5-946f-aea11032172e_en?filename=strategic-dialogue-report-2024_en.pdf.

[11] Irene Canfora, "I giovani agricoltori e l'obiettivo del rinnovo generazionale nella politica agricola comune 2021–27", *Diritto Agroalimentare*, no. 1 (2020): 7; Domenico Cristallo, "I giovani agricoltori al vaglio della Cgue: criticità e prospettive," *Rivista di diritto agrario*, no. 2 (2022): 93; Barbara Zanetti et al., *L'Italia e la Pac post 2020—Policy Brief 7, OS 7: attirare i giovani agricoltori e facilitare lo sviluppo imprenditoriale nelle aree rurali* (Rete Rurale Nazionale, 2020).

[12] Fernando Salaris, "I giovani agricoltori," in *Trattato breve di diritto agrario italiano e comunitario*, ed. Luigi Costato and Alberto Abrami (Cedam, 2003), 241.

the maintenance and enhancement of the territory, and, above all, in the creation of a more competitive and innovative system,[13] which guarantees development of rural areas.

The legal definition of young farmer appears in Art. 4, par. 6, of the Regulation (EU) 2021/2115 of the European Parliament and of the Council of 2 December 2021 establishing rules on support for strategic plans to be drawn up by Member States under the common agricultural policy (CAP Strategic Plans) and financed by the European Agricultural Guarantee Fund (EAGF) and by the European Agricultural Fund for Rural Development (EAFRD) and repealing Regulations (EU) No 1305/2013 and (EU) No 1307/2013.[14] In this article, it is established that, in line with the role entrusted to the Member States in achieving the objectives, the definition must be determined by each individual State in the strategic plans of the CAP. In fact, "'Young farmer' shall be determined in such a way as to include: (a) an upper age limit set between 35 years and 40 years; (b) the conditions for being 'head of the holding'; (c) the appropriate training or skills required, as determined by Member States."

The Regulation (EU) No. 2021/2115, establishing rules on support for strategic plans to be drawn up by Member States under the Common Agricultural Policy (CAP Strategic Plans) and financed by the European Agricultural Guarantee Fund (EAGF) and by the European Agricultural Fund for Rural Development (EAFRD), provides a package of general objectives (Art. 5) and focuses on nine specific objectives (Art. 6).

For the purposes of this contribution, Regulation (EU) No. 2021/2115, which contains provisions on supporting strategic plans drafted by Member States, includes among the specific objectives of Article 6, letter (g), the objective of "to attract and support young farmers and new farmers and facilitate sustainable business development in rural areas." To achieve this specific objective, Regulation (EU) 2021/2115 provides two main instruments for Member States: the possibility of introducing complementary income support for young farmers (CIS-YF), financed within the framework of direct payments[15]; and within rural development, the possibility of granting support for the establishment of young farmers and the start-up of new rural businesses (INSTAL).[16]

Furthermore, in the context of generational change policies, Member States can integrate other instruments: support for cooperation for generational change, aimed

[13] Francesco Piras, "Il sostegno ai giovani agricoltori nell'ambito della Pac," *Agriregionieuropa* 14, no. 55 (2018).

[14] OJ L 435, 6.12.2021, pp. 1–186, hereinafter: Regulation (EU) 2021/2115 or reg. (EU) 2021/2115.

[15] Emilio De Meo et al., "Il nuovo sistema dei pagamenti diretti nella riforma della Pac 2023–27," *Rivista di diritto agrario*, no. 2 (2022): 275.

[16] Article 75 reg. (EU) 2021/2115: "Member States shall grant support in the form of lump sums or financial instruments or a combination of both. Support shall be limited to the maximum amount of aid of EUR 100,000 and may be differentiated in accordance with objective criteria."

at encouraging the development of youth entrepreneurship in agriculture through forms of coaching and cooperation between farmers who have achieved retirement age and young people who do not own agricultural land, with the aim of gradually passing the management of the agricultural business activity to young people[17]; investment support for young people or financial instruments with specific rules for young people[18]; training and consultancy for young agricultural entrepreneurs, as part of the so-called Agricultural Knowledge and Innovation System (AKIS)[19]; possible support for generational turnover activated within the Leaders; the possibility for Member States to grant start-up aid for young farmers and start-up aid for agricultural activities, taking into account the particular difficulties that young people encounter in starting an agricultural business.[20]

In line with the European Union framework, the Strategic Plan of Italy defines the strategy to support and attract young people into agriculture through a set of interventions to meet the needs identified under specific objective 7 (SO7), namely "Attirare e sostenere i giovani agricoltori e i nuovi agricoltori e facilitare lo sviluppo imprenditoriale sostenibile nelle zone rurali" (Attract and support young farmers and new farmers and facilitate sustainable entrepreneurial development in rural areas).

The drafting phase of the Strategic Plan of Italy led to the formulation of a single need regarding Specific Objective 7, precisely E3.1: "Promuovere l'imprenditorialità nelle aree rurali favorendo l'ingresso e la permanenza di giovani e di nuovi imprenditori qualificati alla conduzione di aziende agricole, forestali ed extra—agricole, garantendo un'adeguata formazione, facilitando l'accesso al credito ed al capitale fondiario e favorendo la multifunzionalità delle imprese e i processi di diversificazione dell'attività aziendale, la sostenibilità ambientale, l'innovazione e la digitalizzazione dell'azienda" (Promote entrepreneurship in rural areas by encouraging the entry and retention of young and new qualified entrepreneurs in the management of agricultural, forestry, and non-agricultural businesses, ensuring adequate training, facilitating access to credit and land capital, and promoting the multifunctionality of enterprises and the diversification of business activities.)

In light of the performance-based model, the National Strategic Plan associates two result indicators with specific objective 7, chosen from the common ones identified for the strategic objective in question. Specifically, indicator R.36 "Numero di giovani agricoltori che si sono insediati beneficiando del sostegno della PAC" (Number of young farmers who created an agricultural business with the support of

[17] Article 77.6 reg. (EU) 2021/2115.

[18] Article 73.4 reg. (EU) 2021/2115.

[19] Article 78 reg. (UE) 2021/2115.

[20] Article 18 of Regulation (EU) 2022/2472 of the Commission of 14 December 2022 declares the compatibility of such aid with the internal market, pursuant to articles 107, par. 3, letter (c), and 108, par. 3, TFEU. See also the Communication from the Commission "Guidelines for State aid in the agricultural and forestry sectors and in rural areas" (2022/C 485/01).

the CAP), which, in fact, quantifies the new farmers established thanks to support from the CAP. Furthermore, result indicator 36 breaks down new young farmers by gender. The reference to young farmer must be understood as defined pursuant to Art. 4, par. 1, letter (e), reg. (EU) 2021/2115.

Another indicator chosen is R.39 "Numero di imprese rurali, tra cui imprese della bioeconomia, create grazie a finanziamenti a titolo della PAC" (Number of rural agricultural businesses, including bioeconomy businesses, created with the support of the CAP). This indicator quantifies the result by considering the number of agricultural businesses developed with the support of the CAP, not limiting itself to just the new businesses created.

The position of young farmers and the issue of generational turnover are also closely related to specific objective 8 (SO8), which is "Promuovere l'occupazione, la crescita, la parità di genere, inclusa la partecipazione delle donne all'agricoltura, l'inclusione sociale e lo sviluppo locale nelle zone rurali, comprese la bioeconomia circolare e la silvicoltura sostenibile" (To promote employment, growth, gender equality, including the participation of women in agriculture, social inclusion, and local development in rural areas, including the circular bioeconomy and sustainable forestry.)

In this regard, it highlights what has already been previously emphasised regarding policies supporting small agricultural enterprises: all actions undertaken converge towards the same goal, namely preserving the vitality of rural areas to ensure, through their prosperity, the resilience of the entire agri-food sector.[21]

The definition of a young farmer[22] appears in paragraph 4.1.5 of the National Strategic Plan, where, in line with the decisions of Reg. (EU) 2021/2115, it is expected that such an individual meets these requirements:

a) a maximum age limit of 40 years;

b) the conditions for being a company head;

c) adequate training and/or skills requirements.

The strategy for young farmers and generational turnover will be implemented by combining complementary income support for young farmers and rural development intervention for the establishment of young people in agricultural businesses with national tools and initiatives, aimed at encouraging the establishment of young people farmers and accessing to credit and land capital, in order to create the best conditions for the development of new entrepreneurship in rural areas.

[21] Com (2021) 345 final, "A long-term Vision for the EU's Rural Areas—Towards stronger, connected, resilient and prosperous rural areas by 2040", Bruxelles, 30.6.2021.

[22] Nicola Lucifero, "Il "giovane" agricoltore," *Trattato breve di diritto agrario italiano e dell'Unione europea. Agricoltura, pesca, alimentazione e ambiente*, ed. Luigi Costato and Ferdinando Albisinni, 4th ed. (Cedam, 2023), 450.

3. The Measures Included in Law No. 36/2024

It is evident that young farmers play a crucial role in developing and safeguarding the competitiveness of the agricultural sector. Thus , given the issues related to the obstacles they face in accessing the sector, it is essential to consider what possible legal solutions can be implemented.

The Italian legislator, even before enactment of the law in question, had launched regulatory interventions aimed at encouraging the presence of young people and women in the agricultural sector. In particular, among the measures adopted, those concerning land ownership, the provision of subsidised mortgages and agricultural welfare are noteworthy, now as then.

Given the problems linked to the obstacles that young farmers encounter in accessing the sector, we need to ask ourselves what the possible legal solutions are.

The objective of the national strategy under examination is to strengthen the resilience and vitality of rural territories, generating opportunities for new entrepreneurship, especially for the young generations and women, favouring the conditions of access to land and credit, and guaranteeing and recognising the importance of access to training as a tool for acquiring knowledge and skills necessary for innovation and competitiveness in the agricultural sector.

Law no. 36/2024, in this sense, in compliance with and implementing EU legislation, and in consideration of the specific Italian business structure, has the objective of structuring an organic and non-sectoral system of internal rules aiming to integrate and coordinate the instruments already in place in favour of young farmers, in order to promote, support and relaunch youth entrepreneurship in the agricultural sector.

The range of tools provided by the national legislator includes fiscal-financial measures, such as incentives granted through a dedicated fund to support initial establishment and the provision of a favourable tax regime. Civil law measures include a preferential regime for young farmers in the pre-emption between neighbouring lands, as well as training incentives. Due to the variety of measures contemplated by the law, this is an ambitious project that attempts to address the issue of generational turnover in agriculture from all angles.

Within the law, specifically, Chapter II, dedicated to support the establishment of young people in agriculture ("Sostegno all'insediamento dei giovani nell'agricoltura"), and Chapter III, dedicated to measures aimed at encouraging the retention of young people in the agricultural sector and fostering generational turnover ("Misure per favorire la permanenza dei giovani nel settore agricolo e il ricambio generazionale"), identify appropriate tools to promote youth agricultural entrepreneurship. Chapter IV, which deals with activities related to agricultural labour analysis ("Attività di analisi in materia di lavoro agricolo"), provides for the establishment of the National Observatory for Youth Entrepreneurship and Work in Agriculture, whose

aim is to foster administrative synergies in the field of youth entrepreneurship, also through the coordination between state and regional initiatives.

Article 2 provides a definition[23] of youth agricultural enterprise or young agricultural entrepreneur, understood as an enterprise established in any form, which, exclusively engaging in agricultural activities as defined by Article 2135 of the Italian Civil Code, meets the following conditions: (a) the owner is an agricultural entrepreneur aged over eighteen and under forty-one years old; (b) in the case of partnerships and cooperatives, including the cooperatives referred to in Article 1, paragraph 2, of Legislative Decree 18 May 2001, no. 228, at least half of the partners are agricultural entrepreneurs aged over eighteen and under forty-one years old; (c) in the case of corporations, at least half of the share capital is subscribed by agricultural entrepreneurs aged over eighteen and under forty-one years old, and the administrative bodies are composed, for at least half, of the same individuals.

Article 3 provides for the establishment of a fund, accessible to young agricultural entrepreneurs under 41 years of age, individually or in association, aimed at co-financing programmes prepared by the regions. The resources intend to encourage interventions aimed at: purchasing land and structures necessary for starting agricultural business activities; purchasing capital goods, with priority given to those intended to increase company efficiency and to introduce innovations relating to the product, as well as to the cultivation practices and natural maintenance of the land and to the process of growing the products through precision techniques; expanding the minimum production unit, defined according to location, cultivation direction and use of labour, in order to promote company efficiency.

Outlined below is Art. 4, which contains provisions regarding the preferential tax regime for the first establishment of youth businesses in agriculture, meeting the conditions that the beneficiaries have not carried out any other agricultural business activity in the previous three years and have regularly fulfilled the social security, insurance and administrative obligations envisaged by law and that the benefit does not concern cases relating to cases of transfer of businesses (either in the form of individual businesses or companies) pre-existing to young agricultural entrepreneurs.

A further provision is provided for Article 5, where, for sales contracts concerning the purchase of agricultural land and related appurtenances not exceeding 200,000 euros, reductions have been arranged regarding the compensation for notary activities.

The instruments described can be interpreted in light of the result indicators identified in the National Strategic Plan, such as R.36 "Number of young

[23] Margherita Brunori, *Le qualifiche soggettive dell'imprenditore agricolo. Criteri, evoluzione, prospettive*, (Giappichelli, 2024), 152–57.

farmers who have established an agricultural enterprise with CAP support" and R.39 "Number of rural agricultural enterprises, including bioeconomy businesses, created with CAP support." These instruments, in fact, influence the number of young farmers who, by accessing such support measures, go on to establish an agricultural enterprise.

Particular attention is dedicated to training. In fact, Article 6 recognises the possibility to offer young agricultural entrepreneurs a tax credit equal to 80% of the expenses actually incurred in the year 2024 and, appropriately documented, up to a maximum amount of 2,500 euros for each beneficiary, for participation in training courses relating to the management of the agricultural company.

Article 9 provides the possibility for the regions to offer incentives to associations made up mostly of young people for the management of replacement services in associated companies, as well as providing incentives for maintaining the business unit through the use of the family pact referred to in the articles from 768-bis to 768-octies of the Civil Code.

In line with the AKIS tool foreseen by Art. 78 reg. (EU) 2021/2115, Art. 10 provides for the establishment of the National Observatory for entrepreneurship and youth work in agriculture (ONILGA). This body, composed of representatives of the Ministry of Agriculture, Food Sovereignty and Forestry, the Ministry of Labor and Social Policies, Ismea, the organisations of employers and workers in the agricultural sector and the youth associations operating in the agricultural and agri-food sectors, will be a place for planning, exchanging and disseminating knowledge and innovation, in order to operate in synergy to support the decision-making and problem-solving process in agriculture. Among the many skills are: collecting and processing data relating to the employment possibilities of young people in the agricultural sector and, in general, in rural areas; analysing the legislation concerning youth work and of the interventions carried out by state and regional administrations as well as by the European Union; consultancy and support towards administrations and public bodies for the planning and implementation of initiatives in favour of young people working in the agricultural sector; promoting active policies, rural development policies, support for the organisation and implementation of training experiences and business exchanges, as well as business coaching and tutoring services, for young people, carried out by other agricultural entrepreneurs with suitable requirements and skills.

Lastly, as a further measure aimed at encouraging youth entrepreneurship, the law intervenes, with Art. 11, regarding direct sales. To be precise, paragraph 1 provides that the Municipalities, in the markets for the direct sale of agricultural products carried out in public areas through the use of stands, may reserve for young agricultural entrepreneurs, both in the form of individual and associated enterprises, a share of parking spaces up to 50 percent of their total number.

The young agricultural entrepreneur intervenes directly in the marketing circuit of agri-food products, satisfying his or her own needs and receiving adequate remuneration for work. Indeed, a measure of this type, which values the local dimension, guarantees the appropriation of the profit margin which, otherwise, would be dispersed along the segments of the supply chain.

4. Article 8 "La prelazione di più confinanti" (The Pre-Emption Right of Multiple Neighbors)

Regarding measures aimed at ensuring the retention of young farmers, Article 8 is particularly representative of the legislation in favour of young farmers.

This article, titled "Prelazione di più confinanati" (Pre-emption by Neighbours), introduces a preferential criterion for young entrepreneurs in terms of privileged access to the right of pre-emption for *inter vivos* transactions.[24]

It should be noted that the right of pre-emption for neighbours grants the neighbouring cultivator the right to be preferred over a third party in the transfer of ownership of a rural property. The violation of this preferential right entitles the pretermitted pre-emptive right holder to acquire ownership through the remedy of right of redemption.

Law 36/2024, innovating the previous regulations, repeals article 7 of Legislative Decree no. 18 May 2001. 228, and provides for new preferential criteria in the case of multiple neighbouring subjects, for the purposes of exercising the right of pre-emption pursuant to Art. 7 of the Law of 14 August 1971 no. 817,[25] of the right of redemption referred to in Art. 8, fifth paragraph, of the Law of 26 May 1965 no. 590[26] and of the right of pre-emption in the disposal and leasing procedures referred to in the Art. 66, third paragraph, of the legislative decree of 24 January 2012 no. 1.

Article 8 of Law No. 36/2024 establishes new criteria for resolving the competition for pre-emption or redemption by multiple eligible parties, stipulating that preference is given to the individuals mentioned in Article 2, paragraph 1: namely, agricultural entrepreneurs aged over eighteen and under forty-one years old (letter (a)), partnerships and cooperatives in which at least half of the members are agricultural entrepreneurs within the same age range (letter (b)), and corporations

[24] Referring in this case to agricultural pre-emption. Given that the pre-emptions can be divided into voluntary or legal, among the latter we note those in the field of inheritance (732 Civil Code), regarding the succession in agricultural contracts (articles 48 and 49, L. 3 May 1982, no. 203); in leases (articles 38 and 39, Law 27 July 1978, no. 392); in company law (Art. 2469 Civil Code); in the family business (Art. 230 bis of the Civil Code).

[25] Pre-emption of the owner of the land bordering the one offered for sale.

[26] Pre-emption granted to the tenant of the property offered for sale.

in which at least half of the share capital is held by agricultural entrepreneurs within the same age range and the administrative bodies are composed, for at least half, of the same individuals (letter (c)).

Additionally, among these subjects, the law recognises a further order of priority, preferring young agricultural entrepreneurs as per letter (a),[27] followed by youth agricultural enterprises as per letters (b) and (c).

In cases of equal conditions among neighbours, preference will be given to the party possessing adequate knowledge and skills according to Article 4, paragraph 6, of Regulation (EU) 2021/2115.

This provision can be seen as confirming the legislator's intent to ensure the continuation of activity on the specific property subject to pre-emption or redemption by a young person, whether a natural or legal person.

Furthermore, by recognising possession of adequate knowledge and skills as a residual criterion of preference, it underscores the importance of ensuring an agri-food system that comprises educated young farmers, thus being modern, efficient, and innovative. It should be added that the pre-emption right of the young farmer in the case of multiple neighbours should reduce disputes in this area and, consequently, facilitate the growth of business capital through access to land and expansion of areas. Thus, Article 8 frames the legislative intent to consolidate young agricultural enterprises and support generational turnover in agriculture.

Summary

The examination of the contents of Law No. 36/2024 prompts several considerations. Young Italian—and European—farmers encounter multiple barriers to entry into the agricultural sector. To ensure generational turnover, an economic support policy for young people is necessary, based on a fairer distribution of resources, and providing greater support to young small and medium-sized enterprises, as well as recognising their key role in terms of production functions and supply of goods for the community.

Furthermore, merely providing economic support to young farmers is not sufficient. It is necessary to implement targeted measures for generational turnover that, in the long term, operate stably and systematically.

It therefore emerges that several factors influence generational turnover. For this reason, the objective of attracting young farmers to rural areas must be considered from a broader perspective, and the policy for generational turnover must be an integral part of a general agricultural policy direction, aiming not only to offer

[27] In practice, Art. 8 provides for a preference criterion that favours the natural person, making the individual prevail over partnerships and corporations.

measures to incentivise the entry of young people but also to structure a competitive agri-food system as a whole, capable of ensuring a reasonable level of remuneration and guaranteeing the resilience of agricultural activities.[28]

The critical challenges related to generational turnover require intervention on certain legal institutions to guarantee generational transition in agriculture and facilitate the settlement of young people. One example is the right of pre-emption for neighbours. This legal instrument directly impacts land ownership and access. In doing so, it supports young farmers during the phases of starting and expanding their agricultural enterprises, while also encouraging them to remain in the sector. Indirectly, it also supports the modernisation and innovation of infrastructure, as well as competitiveness, recognising that a young head of the company brings added value to their enterprise and to rural communities.

In this perspective, Member States, also through the flexibility afforded by the new CAP implementation model, may develop strategies that take into account the needs of young farmers in connection with the specificities of the national territory.

Therefore, interventions must also include measures to improve the position of young farmers along the agri-food supply chain and ensure the removal of obstacles that hinder young people' access to and retention in the sector.

In this context, the recent Italian Law no. 36/2024 on the promotion and development of youth entrepreneurship in the agricultural sector, aiming to be an integrated rather than a sectoral intervention, seeks to structure an organic system of internal regulations. This is intended to supplement and coordinate existing tools in favour of young farmers by providing measures to facilitate the entry and retention of young people in agriculture, thus enhancing the vitality and resilience of the entire agri-food sector.

As a result, Law No. 36/2024, which addresses multiple areas—financial, fiscal, and civil—serves as a starting point for constructing a comprehensive support policy for young farmers, on whom the future of the agricultural production sector depends.

BIBLIOGRAPHY

Bolognini, Silvia. "La comunicazione della Commissione europea "Il futuro dell'alimentazione e dell'agricoltura"." *Rivista di diritto agrario*, no. 1 (2018): 110–35.

Brunori, Margherita. *Le qualifiche soggettive dell'imprenditore agricolo. Criteri, evoluzione, prospettive*. Giappichelli, 2024.

Canfora, Irene. "I giovani agricoltori e l'obiettivo del rinnovo generazionale nella politica agricola comune 2021–27." *Diritto Agroalimentare*, no. 1 (2020): 7–22.

[28] Nicola Lucifero, "Imprese agricole e start-up tra innovazione e ricambio generazionale," in *Start-up e PMI innovative in agricoltura. Le imprese agricole tra innovazione e sostenibilità*, ed. Mario Mauro (Cedam, 2024), 44.

Canfora, Irene. "Raggiungere un equilibrio nella filiera agroalimentare. Strumenti di governo del mercato e regole contrattuali." In *Cibo e diritto. Una prospettiva comparata: Volume 1*, edited by Lucia Scaffardi and Vincenzo Zeno-Zencovich. Roma TrE-Press, 2020.

Carbone, Anna, Alessandro Corsi, and Franco Sotte. "La misura giovani tra nuovo Regolamento sullo sviluppo rurale e prime evidenze dell'applicazione 2000–2003." *Agriregionieuropa* 1, no. 2 (2005).

Costantino, Laura. "La problematica dei prezzi dei prodotti agricoli: strumenti normativi tra antichi problemi e nuove crisi." *Rivista di diritto agrario*, no. 2 (2020): 783–99.

Cristallo, Domenico. "I giovani agricoltori al vaglio della Cgue: criticità e prospettive." *Rivista di diritto agrario*, no. 2 (2022): 93–106.

De Meo, Emilio, Rocco Roma, and Annalisa De Boni. "Il nuovo sistema dei pagamenti diretti nella riforma della Pac 2023–27." *Rivista di diritto agrario*, no. 2 (2022): 274–88.

Lattanzi, Pamela. "Le dimensioni aziendali nelle scelte della nuova Pac: le piccole aziende agricole." *Rivista di diritto agrario*, no. 2 (2022): 180–215.

Lucifero, Nicola. "Il "giovane" agricoltore." In *Trattato breve di diritto agrario italiano e dell'Unione europea. Agricoltura, pesca, alimentazione e ambiente*, edited by Luigi Costato and Ferdinando Albisinni, 4th ed. Cedam, 2023.

Lucifero, Nicola. "Imprese agricole e start-up tra innovazione e ricambio generazionale." In *Start-up e PMI innovative in agricoltura. Le imprese agricole tra innovazione e sostenibilità*, edited by Mario Mauro. Cedam, 2024.

Piras, Francesco. "Il sostegno ai giovani agricoltori nell'ambito della Pac." *Agriregionieuropa* 14, no. 55 (2018).

Salaris, Fernando. "I giovani agricoltori." In *Trattato breve di diritto agrario italiano e comunitario*, edited by Luigi Costato and Alberto Abrami. 3rd ed. Cedam, 2003.

Sotte, Franco, Anna Carbone, and Alessandro Corsi. "Giovani e impresa in agricoltura." *Agriregionieuropa* 1, no. 2 (2005).

Zanetti, Barbara, Francesco Piras, and Davide Longhitano. *L'Italia e la Pac post 2020—Policy Brief 7, OS 7: attirare i giovani agricoltori e facilitare lo sviluppo imprenditoriale nelle aree rurali*. Rete Rurale Nazionale, 2020.

ZESZYT PRAWNICZY UAM
NR 15/2025
https://doi.org/10.14746/zpuam.2025.15.8

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

JAKUB SAWICKI

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0000-6591-4979
jaksaw2@st.amu.edu.pl

The Role of Decision-Making Algorithms in Public Administration—Legal and Ethical Challenges

Abstract: The increasing reliance on decision-making algorithms in public administration raises significant legal and ethical challenges. This article examines the key issues associated with algorithmic governance, including transparency, accountability, and potential biases in automated decision-making processes. Using a legal-analytical method, I evaluate whether machine-learning algorithms can comply with existing legal principles while enhancing efficiency in governance. My findings suggest that while algorithms can improve decision-making speed and accuracy, their nature complicates compliance with legal transparency and due process requirements. I argue that algorithmic accountability mechanisms, including explainability frameworks and regulatory oversight, are essential in order to ensure fairness and legality in automated administrative decisions.

Keywords: algorithmic governance, public administration, transparency, accountability, artificial intelligence

Introduction

The integration of decision-making algorithms into public administration has significantly transformed governmental processes by enhancing operational efficiency, streamlining bureaucratic workflows, and improving the accuracy of predictive analytics.[1] These technologies enable authorities to rapidly analyse vast amounts of data, allowing for more informed policy-making, optimized resource allocation, and improved service delivery.[2] However, while these advancements present numerous benefits, their adoption also raises critical concerns regarding transparency, fairness, and legal accountability, particularly in the context of democratic governance.[3] One of the most pressing challenges is the "black-box" nature of machine-learning models, which often operate through complex, opaque processes that make it difficult for both citizens and oversight bodies to scrutinize administrative decisions.[4] This

[1] Cary Coglianese and David Lehr, "Transparency and Algorithmic Governance," *Administrative Law Review* 71, no. 1 (2019): 6–8.

[2] Michael Veale and Lilian Edwards, "Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling," *Computer Law & Security Review* 34, no. 2 (2018): 398–99, https://doi.org/10.1016/j.clsr.2017.12.002.

[3] Joshua A. Kroll et al., "Accountable Algorithms," *University of Pennsylvania Law Review* 165, no. 3 (2017): 638–39.

[4] Tal Zarsky, "The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making," *Science, Technology, & Human Values* 41, no. 1 (2016): 121–22, https://doi.org/10.1177/0162243915605575.

lack of interpretability can undermine the principles of due process, as affected individuals may struggle to understand the rationale behind automated decisions that impact their rights, benefits, or obligations. Without adequate explainability, these systems risk eroding public trust in governmental institutions and exacerbating concerns about algorithmic bias and discrimination.[5] Furthermore, the deployment of algorithmic decision-making at scale within public institutions introduces broader implications for democratic legitimacy and social acceptance. The reliance on data-driven governance models necessitates critical examination of whether these systems align with constitutional principles, including equal protection under the law, non-discrimination, and procedural fairness. Issues such as algorithmic bias, the disparate impact on marginalized communities, and the reinforcement of existing social inequalities must be carefully addressed to ensure that these technologies do not perpetuate or exacerbate systemic injustices.[6] Additionally, concerns extend beyond legal and ethical considerations to include the fundamental question of human oversight in automated decision-making. The risk of "automation bias", where public officials defer excessively to algorithmic outputs without critically assessing their validity, further complicates the landscape of responsible AI implementation in public administration.[7] Effective regulatory interventions, such as independent audits, algorithmic impact assessments, and mechanisms for contestability and redress, must be established to ensure accountability and compliance with democratic values. Given these complexities, policymakers, legal scholars, and technologists must engage in an interdisciplinary dialogue to develop robust frameworks that balance efficiency gains with the protection of fundamental rights. Addressing these concerns requires a multi-faceted approach, including legislative measures, ethical AI guidelines, and participatory mechanisms that allow stakeholders, including the public, to be involved in the governance of algorithmic systems. Only through comprehensive regulation and governance can the full potential of algorithmic decision-making be harnessed in a manner that upholds principles of transparency, fairness, and democratic integrity.[8]

---

[5] Danielle Keats Citron and Frank Pasquale, "The Scored Society: Due Process for Automated Predictions," *Washington Law Review* 89, no. 1 (2014): 24–25.

[6] Karen Hao, "This Is How AI Bias Really Happens—and Why It's So Hard to Fix," MIT Technology Review, published 4 February 2019, https://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/.

[7] James Vincent, "The Problem with AI Ethics," The Verge, published 3 April 2019, https://www.theverge.com/2019/4/3/18293410/ai-artificial-intelligence-ethics-boards-charters-problem-big-tech.

[8] Sandra Wachter et al., "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law* 7, no. 2 (2017): 76–99, https://doi.org/10.1093/idpl/ipx005.

1. Legal Principles Governing Algorithmic Decision-Making

1.1. Transparency and Explainability

Transparency in government decision-making is a fundamental principle enshrined in democratic governance, ensuring that public institutions operate with openness and accountability.[9] Transparent governance fosters trust between citizens and the state, reinforcing the legitimacy of administrative actions. It allows individuals to understand how decisions that affect their rights, obligations, and access to services are made. The legal concept of "fishbowl transparency" requires that government decisions be subject to public scrutiny, making all relevant information available to ensure accountability.[10] This means that the reasoning, data, and methodologies used in administrative decision-making must be accessible to the public, stakeholders, and oversight bodies. On the other hand, "reasoned transparency" necessitates providing explicit justifications for administrative actions, ensuring that decisions are not made arbitrarily or without proper explanation.[11] In essence, reasoned transparency demands that government agencies articulate the basis for their decisions, whether they result in policy implementation, law enforcement, or the allocation of public resources. However, the widespread adoption of machine-learning algorithms in public administration poses significant challenges to these transparency principles. Many of these algorithms function as "black boxes", meaning that even their developers may struggle to explain how specific decisions are reached. The complexity of artificial intelligence (AI) models, particularly deep learning systems, creates barriers to public understanding and legal compliance.[12] Without adequate transparency, there is a risk that automated decisions may lead to unfair, biased, or erroneous outcomes without affected individuals being able to challenge or understand them. To address these challenges, governments must develop robust explainability frameworks which ensure that algorithms used in public administration can be scrutinized and understood. One approach involves implementing model interpretability techniques, which enable the dissection of AI-driven decision-making processes. These techniques include rule-based explanations, feature importance analysis, and counterfactual reasoning, which help illustrate how different factors influence algorithmic outputs. Another approach is open auditing of algorithmic decisions, allowing external experts, policymakers, and civil society organizations to

[9] Coglianese and Lehr, "Transparency and Algorithmic Governance," 20–21.

[10] Gardner Susan Marie, "Accountability, Transparency, and Living in the Fishbowl," Municipal World, published March 2019, https://www.municipalworld.com/feature-story/life-in-fishbowl/.

[11] Lilian Edwards and Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For," *Duke Law & Technology Review* 16, no. 1 (2017): 38–40.

[12] Zarsky, "The Trouble with Algorithmic Decisions," 126–28.

assess the fairness, accuracy, and reliability of AI-driven decision-making systems.[13] Explainability is particularly crucial in high-stakes applications, where algorithmic decisions have significant consequences for individuals and society. For example, in social welfare benefits allocation, automated systems determine eligibility and distribute resources to citizens in need. Lack of transparency in these systems can lead to unjustified denials or reductions of benefits, disproportionately affecting vulnerable populations. Similarly, in the criminal justice system, risk assessment algorithms are often used to predict recidivism rates or recommend sentencing outcomes. Without clear explanations of how these decisions are made, individuals may face wrongful classifications that impact their freedom and future opportunities. Ensuring transparency and explainability in government decision-making requires a multi-faceted approach. Governments must not only implement technical solutions to enhance AI interpretability but also establish legal frameworks mandating disclosure and justification of algorithmic decisions. Public officials should receive specialized training to critically assess algorithmic outputs and ensure that decisions are subject to human oversight. Furthermore, citizen engagement and participatory governance mechanisms should be promoted to allow the public to contribute to discussions on the ethical deployment of AI in administration. By prioritizing transparency and explainability, governments can maintain public trust, uphold democratic values, and mitigate the risks associated with opaque decision-making processes.[14] A clear regulatory framework combined with technological advancements in AI interpretability can help ensure that decision-making algorithms serve the public interest while safeguarding individual rights and freedoms.

1.2. Due Process and Accountability

Administrative law mandates that individuals subject to governmental decisions must receive an explanation and an opportunity to contest the outcome. This principle is deeply rooted in democratic governance and ensures that state authorities remain accountable for their actions. It serves as a safeguard against arbitrary decision-making, reinforcing the rule of law and protecting citizens from unjustified administrative actions.[15] As public institutions increasingly rely on automated decision-making systems, the challenge lies in ensuring that these fundamental principles remain upheld, even in cases involving AI and machine-learning algorithms. The European General Data Protection Regulation (GDPR) explicitly addresses the risks associated with automated decision-making, particularly in cases where such

[13] Wachter et al., "Why a Right to Explanation of Automated Decision-Making Does Not Exist," 76–99.

[14] Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact," *California Law Review* 104, no. 3 (2016): 729–31, http://dx.doi.org/10.15779/Z38BG31.

[15] Citron and Pasquale, "The Scored Society," 13–14.

decisions may have significant legal or personal consequences.[16] Article 22 of the GDPR limits fully automated decision-making processes that result in legal effects or similarly significant impacts. However, the applicability of Article 22(3)—which mandates safeguards such as human intervention, the right to express views, and the right to contest decisions—is limited to cases where the automated decision is either necessary for the performance of a contract or based on the explicit consent of the data subject (Article 22(2)(a) and (c) GDPR). These conditions are rarely met in public administration contexts, where decisions are typically based on legal mandates (Article 22(2)(b)). In such cases, the regulation merely requires "appropriate safeguards", without detailing specific mechanisms.[17]

Moreover, Article 22 must be interpreted in conjunction with other provisions of the GDPR, including Article 13(2)(f), Article 14(2)(g), and Article 15(1)(h), which establish transparency obligations concerning the logic, significance, and consequences of automated decisions.[18] These complementary provisions form an integrated framework for ensuring data subject awareness and agency. Beyond the GDPR, the recently adopted Artificial Intelligence Act (AI Act, August 2024) provides additional requirements, particularly Article 86, which imposes duties of transparency and explainability for high-risk AI systems.[19] This includes the obligation to provide understandable information about how AI systems function and how decisions are made. Notably, Article 86(3) stresses that these obligations must be read in light of existing Union and Member State law, creating a layered framework of interrelated norms.

Therefore, a comprehensive legal assessment must go beyond Article 22 GDPR and include the AI Act as well as relevant national provisions, such as Germany's *Verwaltungsverfahrensgesetz* (Administrative Procedure Act), which already incorporates safeguards for automated decision-making processes.[20] The failure to acknowledge this broader legal landscape significantly undermines the robustness of legal analysis. While the article correctly calls for "comprehensive legal frameworks that go beyond the basic protections outlined in GDPR," it overlooks existing

[16] 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) (OJ L 119, 4.5.2016, pp. 1–88).

[17] Andrew D. Selbst and Julia Powles, "Meaningful Information and the Right to Explanation," *International Data Privacy Law* 7, no. 4 (2017): 233–42, https://doi.org/10.1093/idpl/ipx022.

[18] Wachter et al., "Why a Right to Explanation of Automated Decision-Making Does Not Exist," 76–99.

[19] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024).

[20] Karen Yeung, "Algorithmic Regulation: A Critical Interrogation," *Regulation & Governance* 12, no. 4 (2018): 520–23, https://doi.org/10.1111/rego.12158.

instruments that already begin to address these challenges. A complete evaluation must critically assess whether the current legal regime—including the GDPR, AI Act, and national administrative law—is sufficient or requires enhancement.

Another critical issue relates to the lack of human oversight in algorithmic decision-making. While GDPR requires meaningful human intervention in high-stakes automated decisions, the practical implementation of this safeguard remains inconsistent across jurisdictions. In many cases, human oversight is either superficial or non-existent, leading to what has been described as automation bias—a phenomenon where human reviewers over-rely on algorithmic outputs without critically assessing their validity.[21] This is particularly problematic in areas such as social welfare allocation, immigration decisions, predictive policing, and risk assessment in the criminal justice system, where algorithmic errors can result in wrongful denials of rights, unjustified penalties, or disproportionate targeting of marginalized communities. To address these challenges, there is an urgent need for comprehensive legal frameworks that go beyond the basic protections outlined in GDPR.

Governments should adopt strict transparency requirements mandating that public institutions disclose the logic, criteria, and datasets underlying algorithmic decisions. Additionally, independent oversight mechanisms—such as external audits, algorithmic impact assessments, and specialized regulatory agencies—should be established to monitor the fairness, accuracy, and legality of AI-driven decision-making processes. Such oversight must also include mechanisms for redress, allowing individuals to effectively appeal and rectify erroneous or unjust algorithmic decisions. Furthermore, ensuring due process in algorithmic governance requires greater public participation in the design and deployment of AI-driven systems. Civil society organizations, legal scholars, and technical experts should be actively involved in assessing the potential risks of these technologies before they are implemented in critical areas of public administration. Democratic accountability also demands that policymakers engage in open discussions with affected communities to better understand their concerns and ensure that AI systems are aligned with human rights principles.

2. Ethical Challenges in Algorithmic Public Administration

2.1. Bias and Discrimination

Algorithmic decision-making, while often perceived as objective and data-driven, can inadvertently reinforce and even exacerbate biases present in historical data. These biases may stem from systemic inequalities embedded in past decision-making processes, social prejudices, or institutional discrimination that have historically disad-

[21] Yeung, "Algorithmic Regulation," 505–23.

vantaged certain demographic groups.[22] When machine-learning models are trained on biased datasets, they tend to learn and replicate those biases, leading to algorithmic outcomes that disproportionately affect marginalized communities.[23] One of the most prominent examples of this phenomenon is the use of algorithmic risk assessments in the criminal justice system. Predictive models are frequently employed to assess the likelihood of recidivism, determine bail eligibility, or guide sentencing decisions.[24] However, studies have shown that these algorithms can systematically classify individuals from minority backgrounds as higher-risk compared to their white counterparts, even when controlling for similar offence histories.[25] Such discriminatory outcomes undermine the principles of fairness and equal treatment under the law, leading to concerns about due process violations and systemic racial bias. This issue is further exacerbated when training data reflect historical prejudices, as they encode patterns of past discrimination into automated decision-making. For example, if a hiring algorithm is trained on historical employment data from industries with a long history of gender discrimination, the algorithm may systematically disadvantage female applicants by replicating past hiring biases.[26] Similarly, predictive policing algorithms trained on crime data from neighbourhoods that have been over-policed in the past may perpetuate a cycle of excessive law enforcement targeting those communities, reinforcing existing inequalities. Beyond technical solutions, policy interventions and legal frameworks play a crucial role in mitigating algorithmic bias. Governments and regulatory bodies should enforce transparency and accountability measures, requiring institutions that use algorithmic decision-making to conduct regular bias audits and report on fairness metrics. Additionally, public participation and oversight mechanisms should be implemented to allow affected communities to voice concerns and provide feedback on the fairness of automated decision-making processes.[27]

2.2. The Risk of "Automation Bias"

As public administration increasingly integrates artificial intelligence and machine-learning models into decision-making processes, concerns regarding au-

[22] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown, 2016), 151–53.

[23] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin's Press, 2018), 80–82.

[24] Rashida Richardson et al., "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," *New York University Law Review Online* 94, 2019: 193–95.

[25] Eubanks, *Automating Inequality*, 90.

[26] Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research* 81, 2018: 84–85.

[27] United Nations Human Rights Office, "B-Tech Project Report: Human Rights Risks in AI-Based Decision Making," 2021, https://www.ohchr.org/sites/default/files/documents/issues/business/b-tech/taxonomy-GenAI-Human-Rights-Harms.pdf, accessed 27 February 2025.

tomation bias have become more pronounced.[28] Automation bias refers to the cognitive tendency of human decision-makers, including public officials, to place excessive trust in algorithmic recommendations, often without critically assessing their validity, accuracy, or potential biases. This overreliance can lead to the unquestioned acceptance or rubber-stamping of flawed algorithmic outputs, reducing the role of meaningful human oversight in governance.[29] One of the major risks of automation bias is that it can create a false perception of objectivity in decision-making. Algorithms, though often perceived as neutral and data-driven, may still inherit biases from historical data or flawed training methodologies.[30] When government officials assume that algorithmic outputs are inherently more accurate than human judgments, they may fail to recognise instances where the system produces errors or reinforces structural inequalities. This is particularly concerning in high-stakes scenarios, such as social welfare allocation, law enforcement and criminal justice, and public sector hiring.[31] The consequences of unchecked automation bias extend beyond individual cases of injustice. Over time, its systemic effects can erode public trust in government institutions, particularly when citizens perceive that algorithmic decisions lack transparency, fairness, or accountability.[32] If people believe that AI-driven decisions cannot be challenged or that human officials merely serve as passive enforcers of algorithmic outputs, faith in democratic governance may weaken. To address these challenges, governments must implement comprehensive training programs for public officials, ensuring that they develop the skills necessary to critically evaluate and question algorithmic recommendations.[33] Additionally, government agencies should establish accountability mechanisms, such as mandatory human review of AI-driven decisions, independent audits of algorithmic systems, and accessible appeal processes for citizens affected by automated outcomes. By proactively addressing automation bias, public administrations can harness the benefits of AI while ensuring that algorithmic governance remains aligned with the principles of fairness, transparency, and human-centred decision-making.[34]

---

[28] O'Neil, *Weapons of Math Destruction*, 100.

[29] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, 2015), 216–17.

[30] Yeung, "Algorithmic Regulation," 520–23.

[31] Richardson et al., "Dirty Data, Bad Predictions," 201–05.

[32] Julia Angwin et al., "Machine Bias," ProPublica, published 23 May 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[33] Brent Mittelstadt et al., "The Ethics of Algorithms: Mapping the Debate," *Big Data & Society* 3, no. 2 (2016): 8–10, https://doi.org/10.1177/2053951716679679.

[34] Ann Florini, *The Right to Know: Transparency for an Open World* (Columbia University Press, 2007), 210–12.

3. Proposals for Regulatory and Policy Reforms

As public administration increasingly adopts algorithmic decision-making systems, ensuring algorithmic transparency becomes a fundamental priority for regulatory bodies and policymakers. Transparency in this context means that government agencies must not only disclose the existence of AI-driven decision-making tools but also provide meaningful insights into their underlying logic, data sources, and performance metrics.[35] Without such transparency, citizens and oversight bodies may struggle to assess the fairness, accountability, and reliability of automated administrative decisions. A multilayered transparency approach should be implemented to address different aspects of AI-driven decision-making.

Government institutions should be required to publish clear explanations of how algorithms generate decisions, including the key factors influencing the outcomes. This would help prevent situations where individuals are adversely affected by opaque automated rulings without any recourse to understanding why.[36] The adoption of explainable AI (XAI) techniques, such as interpretable machine learning models, counterfactual explanations, and rule-based decision-making processes, should be prioritized. These methods help bridge the gap between algorithmic efficiency and the need for accountability by making automated decisions more understandable to both policymakers and affected individuals.[37]

Public institutions using AI should, to the extent legally permissible, disclose relevant characteristics of the datasets that train their models. Full disclosure may be constrained by data protection regulations, such as the GDPR, or by confidentiality obligations and trade secrets.[38] The AI Act also introduces provisions restricting the use and disclosure of personal data in high-risk systems, particularly when data subjects cannot be sufficiently anonymized.[39] Therefore, transparency obligations must be balanced against privacy and intellectual property considerations, requiring nuanced implementation strategies. Public scrutiny of training data can help ensure fairness and reduce discriminatory outcomes.[40] To build public trust in AI-driven governance, regulatory frameworks should require institutions to document and publicly disclose validation metrics used to assess algorithmic fairness and reliability. These metrics should include assessments of bias detection, predictive accuracy across different population groups, and evaluations of unintended discriminatory effects.[41] Algorithmic transparency should not be limited to retrospective analysis;

[35] Pasquale, *The Black Box Society*, 215–16.

[36] Selbst and Powles, "Meaningful Information and the Right to Explanation," 233–42.

[37] Yeung, "Algorithmic Regulation," 505–23.

[38] Pasquale, *The Black Box Society*, 219–20.

[39] AI Act.

[40] Reuben Binns, , "Fairness in Machine Learning: Lessons from Political Philosophy," *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency* 81, 2018: 157–58.

[41] Eubanks, *Automating Inequality*, 220–21.

there should also be mechanisms for ongoing audits and real-time monitoring of automated decision-making processes. Additionally, government agencies must implement clear appeal procedures that allow individuals to challenge decisions made by algorithms, thereby ensuring that automated rulings are not final and unreviewable.[42]

Regulatory bodies should enact legislation mandating transparency standards for AI deployment in public administration. Such laws should specify the types of information that must be disclosed, establish mandatory oversight mechanisms, and outline penalties for non-compliance. Moreover, governments should consider establishing independent AI ethics commissions tasked with evaluating the societal impacts of algorithmic decision-making and ensuring compliance with transparency requirements.[43] By institutionalizing these transparency measures, governments can foster greater public trust in AI-driven decision-making, uphold democratic principles, and mitigate risks associated with opaque, unaccountable, and potentially biased automated systems.

It is important to note that since the drafting of this article, the European Union has adopted the Artificial Intelligence Act (August 2024), which addresses several of the concerns raised herein. In particular, the AI Act codifies obligations regarding transparency, documentation, and oversight for high-risk AI systems used in public administration.[44] These include requirements for explainability, data governance, and human oversight, thereby partially responding to demands for regulatory clarity and accountability mechanisms. Nonetheless, gaps remain, particularly in relation to participatory governance, appeal rights, and the detailed procedural safeguards required for ensuring due process in administrative contexts.[45] Therefore, while the AI Act represents a significant step forward, it does not fully obviate the need for continued legal development and empirical evaluation of its implementation.

4. Independent Oversight and Audits

As governments increasingly integrate AI and machine learning algorithms into public administration, the need for independent oversight and auditing mechanisms has never been more critical. Without robust evaluation frameworks, algorithmic decision-making systems may operate with unchecked bias, opacity, and a lack of accountability, leading to potential injustices and public distrust in automated governance.[46] To address these concerns, comprehensive external audits and oversight

[42] United Nations Human Rights Office, "B-Tech Project Report," 10.
[43] Binns, "Fairness in Machine Learning," 159.
[44] AI Act.
[45] Mittelstadt et al., "The Ethics of Algorithms," 7–8.
[46] Yeung, "Algorithmic Regulation," 505–23.

mechanisms must be established to ensure that AI-driven decision-making adheres to legal, ethical, and democratic principles. A multi-layered independent oversight approach should cover several areas.

Regulatory agencies should create independent institutions specifically tasked with auditing government-deployed AI systems. These institutions should have the authority to assess the fairness, accuracy, and transparency of automated decision-making models, ensuring they do not discriminate against vulnerable populations or reinforce systemic biases.[47] Judicial oversight should be integrated into the deployment of AI in public administration. Courts—particularly administrative courts—must be empowered to review whether algorithmic decisions comply with constitutional rights, due process, and administrative law principles.[48] In jurisdictions where administrative decisions are reviewed by specialized courts, these bodies should be equipped to conduct substantive review of algorithmic reasoning and procedural fairness. This may necessitate the adaptation of evidentiary rules to allow for the presentation and critical assessment of algorithmic outputs. In some cases, enabling limited discovery or expert testimony may be necessary to ensure effective judicial oversight.[49] This includes evaluating whether affected individuals have access to meaningful recourse and ensuring that government agencies uphold transparency requirements.[50]

Algorithmic systems should be subject to periodic external evaluations conducted by independent researchers, civil society organisations, and academic institutions. These evaluations should analyse algorithmic fairness, predictive accuracy, and unintended consequences, ensuring that AI tools are aligned with ethical and legal standards.[51] Governments should consider establishing specialized regulatory agencies dedicated to overseeing the deployment of AI in public administration. These agencies should provide domain-specific expertise in algorithmic governance, data ethics, and human rights law, ensuring that AI implementations are equitable, accountable, and socially beneficial.

Beyond technical and legal evaluations, public participation should also play a crucial role in AI oversight. Government agencies should establish transparent feedback channels, allowing affected citizens and advocacy groups to report concerns, provide input on AI policies, and contribute to shaping AI governance frameworks. By involving diverse stakeholders in algorithmic oversight, governments can foster greater trust and inclusivity in AI-driven decision-making.[52] To institutionalize

[47] Mittelstadt et al., "The Ethics of Algorithms," 9–10.

[48] Kroll, "Accountable Algorithms," 633–705.

[49] Coglianese and Lehr, "Transparency and Algorithmic Governance," 23.

[50] "B-Tech Project Report."

[51] Brent Mittelstadt, "Principles Alone Cannot Guarantee Ethical AI," *Nature Machine Intelligence* 1, no. 11 (2019): 501–07, https://doi.org/10.1038/s42256-019-0114-4.

[52] Yeung, "Algorithmic Regulation," 505–23.

these oversight mechanisms, legislative mandates should be introduced to require public-sector AI systems to undergo independent audits before deployment and at regular intervals post-implementation. Non-compliance with these requirements should result in penalties or restrictions on the use of automated decision-making tools, reinforcing the necessity for ethical AI governance. By implementing independent oversight and audit frameworks, governments can mitigate the risks of algorithmic bias, enhance transparency, and safeguard public trust in AI-driven governance. A well-regulated AI ecosystem will ensure that technology serves democratic values, human rights, and social equity, rather than reinforcing existing inequalities or operating in an unaccountable manner.[53]

Summary

The adoption of decision-making algorithms in public administration presents both opportunities and challenges. While AI can enhance efficiency, streamline bureaucratic processes, and improve policy implementation, it also raises concerns regarding bias, transparency, accountability, and due process. Without adequate safeguards, algorithmic decision-making may reinforce systemic biases, undermine public trust, and erode democratic oversight. To address these risks, governments must implement strong transparency measures, including explainability frameworks, open data disclosure, and fairness assessments. The risk of automation bias underscores the importance of human oversight and specialized training for public officials to critically engage with AI-generated recommendations. Moreover, independent audits and regulatory oversight are crucial to ensuring that AI-driven governance complies with constitutional principles and ethical standards. Moving forward, a multi-faceted regulatory approach that includes mandatory audits, judicial review mechanisms, and participatory governance is necessary to align AI implementation with fundamental rights and social justice. By embedding transparency, fairness, and accountability into AI governance, policymakers can maximize the benefits of automation while safeguarding public trust and democratic values.

BIBLIOGRAPHY

Barocas, Solon, and Andrew D. Selbst. "Big Data's Disparate Impact." *California Law Review* 104, no. 3 (2016): 671–732. http://dx.doi.org/10.15779/Z38BG31.

Binns, Reuben. "Fairness in Machine Learning: Lessons from Political Philosophy." *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency* 81, 2018: 149–59.

[53] "B-Tech Project Report."

Buolamwini, Joy, and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of Machine Learning Research* 81, 2018: 77–91.

Citron, Danielle Keats, and Frank Pasquale. "The Scored Society: Due Process for Automated Predictions." *Washington Law Review* 89, no. 1 (2014): 1–33.

Coglianese, Cary, and David Lehr. "Transparency and Algorithmic Governance." *Administrative Law Review* 71, no. 1 (2019): 1–56.

Edwards, Lilian, and Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For." *Duke Law & Technology Review* 16, no. 1 (2017): 18–84.

Eubanks, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.* St. Martin's Press, 2018. https://doi.org/10.5204/lthj.v1i0.1386.

Florini, Ann. *The Right to Know: Transparency for an Open World*. Columbia University Press, 2007.

Kroll, Joshua A., Joanna Huey, Solon Barocas et al. "Accountable Algorithms." *University of Pennsylvania Law Review* 165, no. 3 (2017): 633–705.

Mittelstadt, Brent. "Principles Alone Cannot Guarantee Ethical AI." *Nature Machine Intelligence* 1, no. 11 (2019): 501–07. https://doi.org/10.1038/s42256-019-0114-4.

Mittelstadt, Brent, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, and Luciano Floridi. "The Ethics of Algorithms: Mapping the Debate." *Big Data & Society* 3, no. 2 (2016): 1–21. https://doi.org/10.1177/2053951716679679.

O'Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown, 2016.

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press, 2015.

Richardson, Rashida, Jason Schultz, and Kate Crawford. "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice." *New York University Law Review Online* 94, 2019: 192–233.

Selbst, Andrew D., and Julia Powles. "Meaningful Information and the Right to Explanation." *International Data Privacy Law* 7, no. 4 (2017): 233–42. https://doi.org/10.1093/idpl/ipx022.

Veale, Michael, and Lilian Edwards. "Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling." *Computer Law & Security Review* 34, no. 2 (2018): 398–404. https://doi.org/10.1016/j.clsr.2017.12.002.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." *International Data Privacy Law* 7, no. 2 (2017): 76–99. https://doi.org/10.1093/idpl/ipx005.

Yeung, Karen. "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance* 12, no. 4 (2018): 505–23. https://doi.org/10.1111/rego.12158.

Zarsky, Tal. "The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making." *Science, Technology, & Human Values* 41, no. 1 (2016): 118–32. https://doi.org/10.1177/0162243915605575.

ZESZYT PRAWNICZY UAM
NR 15/2025
https://doi.org/10.14746/zpuam.2025.15.9

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

MARIANNA ZAWAL

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0009-0000-4368-296X
marzaw20@st.amu.edu.pl

The Synergy Between European Union Data Protection and Digital Market Regulation

Abstract: This article examines the relationship between the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA), with a particular focus on how gatekeeper obligations affect the legal bases for personal data processing. While Article 6 GDPR provides several lawful grounds, such as consent, necessity for contract performance, and legitimate interests, Article 5(2) DMA significantly restricts gatekeepers' ability to rely on the latter two. The author highlights the increasing regulatory pressure to ensure that consent is freely given, especially in light of EDPB Opinion 08/2024 and the European Commission's April 2025 decision concerning the "consent or pay" model. The analysis reflects the EU's broader effort to reinforce fundamental rights and ensure genuine user autonomy in the context of digital platform regulation.

Keywords: General Data Protection Regulation, Digital Markets Act, consent, user autonomy

Introduction

In recent years, the pace of technological advancement has been unprecedented. When the General Data Protection Regulation (GDPR) entered into force, it was hailed as a groundbreaking step towards safeguarding personal data in the European Union.[1] However, the digital ecosystem has since evolved dramatically. Artificial Intelligence systems have matured from experimental prototypes to widely deployed tools embedded in consumer platforms, while dominant digital platforms—such as Google, Meta, and Amazon—have deepened their role as essential intermediaries in everyday life.

This rapid evolution has exposed the growing gap between law and technology. Although the GDPR introduced comprehensive rules on personal data processing, many of its provisions are ill-suited to addressing the complexities of data-driven business models, especially those built around profiling, behavioural advertising, and algorithmic decision-making. Moreover, the regulation did not anticipate the extent to which digital platforms would accumulate structural power—not merely as data controllers, but as de facto gatekeepers of access to digital markets and information flows.

[1] 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) (OJ L 119, 4.5.2016, pp. 1–88), hereinafter: GDPR.

Recognising this regulatory lag, the European Union has undertaken a series of legislative initiatives aimed at recalibrating the digital legal order. Chief among them are the Digital Markets Act (DMA),[2] the Digital Services Act (DSA),[3] and the recently adopted AI Act.[4] These instruments signal a shift from traditional, reactive forms of data protection and competition enforcement to a more anticipatory and systemic approach. The DMA introduces *ex ante* obligations for designated gatekeepers, aiming to restore contestability and fairness in core platform services. At the same time, the DSA enhances accountability in online content moderation, while the AI Act seeks to govern algorithmic systems according to their societal risks.

This ambitious regulatory agenda has not gone unnoticed internationally. Leading figures in the current administration of the United States have accused the EU of disproportionately targeting American tech giants under the guise of digital regulation. This criticism reflects not only geopolitical tensions but also deeper disagreements about the scope and legitimacy of regulating data, competition, and innovation in digital markets.[5]

Against this background, this article examines the intersection of data protection and competition law in the regulation of gatekeepers, focusing on the evolving role of legal bases for data processing under the GDPR considering the DMA's provisions. It argues that the EU's efforts to impose structural obligations on dominant platforms are both necessary and normatively justified—but that their success depends on resolving underlying legal tensions, particularly regarding the role of user consent, data portability, and the allocation of enforcement competences.

1. The Role and Limits of Consent under the GDPR

Consent remains one of the most prominent legal bases for processing personal data under the GDPR, reflecting the foundational value of informational self-determination in European data protection law. It is often regarded as the most transparent and user-centric form of legitimising data processing, premised on the autonomy of

[2] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, pp. 1–66), hereinafter: DMA.

[3] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, pp. 1–102), hereinafter: DSA.

[4] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024), hereinafter: AI Act.

[5] Aleksandra Wójtowicz, "U.S. and EU Clash over Regulation of Digital Content Moderation," Polski Instytut Spraw Międzynarodowych, published 21 March 2025, https://pism.pl/publications/us-and-eu-clash-over-regulation-of-digital-content-moderation.

the data subject. Article 6(1)(a) GDPR recognises consent as a lawful basis, further elaborated in Article 4(11) and Recital 32, which emphasise the need for consent to be freely given, specific, informed, and unambiguous.

Yet, in practice, the deployment of consent by powerful digital platforms—especially those designated as "gatekeepers" under the DMA—has proven deeply problematic. These entities frequently operate in structurally imbalanced environments, where users are presented with take-it-or-leave-it choices, nudged by manipulative interface designs (so-called "dark patterns"), or deprived of viable alternatives. As a result, consent mechanisms risk becoming formalistic rather than meaningful, undermining the normative premise of voluntariness. Empirical and regulatory findings have confirmed that many gatekeepers have either circumvented the requirement for consent through reliance on alternative legal grounds, such as "legitimate interest," or implemented consent flows that fall short of the GDPR's stringent standard.

Moreover, the economic incentives propelling data-driven platform models create a systemic tension between the ideal of user control and the commercial logic of maximising data extraction. Gatekeepers have a structural interest in steering users toward consenting to broad, bundled processing purposes, often making withdrawal difficult or opaque. This has raised fundamental concerns about whether consent can function effectively in digital ecosystems dominated by a small number of entrenched intermediaries.

The shortcomings in enforcing meaningful consent under the GDPR—especially in environments shaped by data-driven gatekeepers—have underscored the limitations of traditional legal frameworks in addressing structural power asymmetries. Consent, while a cornerstone of the GDPR, has proven challenging to operationalise effectively in practice, particularly when deployed by entities exercising considerable market power.

The European Data Protection Board (EDPB), in its Guidelines 05/2020 on consent, elaborates that valid consent must be obtained through clear affirmative action, and that mechanisms such as pre-ticked boxes or user inactivity cannot be considered sufficient.[6] The CJEU reinforced this interpretation in its *Planet49* ruling (C-673/17), stating unequivocally that consent must involve active behaviour and cannot be presumed.[7] The Court further held that storing or accessing information on a user's device necessitates informed consent, thereby rejecting opt-out models. Importantly, consent must be granular—separately obtained for each distinct processing operation—and capable of being withdrawn without detriment. Controllers are bound by the accountability principle to demonstrate the validity of the consent they collect.[8]

---

[6] European Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679*, Version 1.1 (4 May 2020).

[7] Judgment of the Court of Justice of the European Union of 1 October 2019, *Planet49* (C673/17), ECLI:EU:C:2019:801.

[8] Paweł Barta et al., "Commentary on Article 6," in *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem*

These stringent requirements establish a high threshold for valid consent, particularly when sought by actors with significant market dominance, such as the digital platforms designated as gatekeepers under the Digital Markets Act. The asymmetry in bargaining power between individuals and dominant platforms heightens the risk that consent will not be freely given, informed, or genuinely revocable. In such contexts, the formal appearance of consent may mask de facto coercion or user habituation to unavoidable data practices—issues that traditional data protection mechanisms have struggled to resolve effectively.

Despite ongoing enforcement efforts by national data protection authorities (DPAs) and the European Data Protection Board, the GDPR's architecture has revealed its limitations in confronting systemic abuses at scale. Similarly, classical EU competition law, rooted in ex post enforcement under Articles 101 and 102 TFEU, has proven slow and ill-suited to address the anticipatory and structural dimensions of digital market power. Although notable efforts such as *Bundeskartellamt v. Meta* have introduced privacy into the antitrust discourse, these developments remain fragmented and jurisdictionally constrained.[9]

In response, the European Union introduced the DMA as an *ex ante* regulatory regime tailored to the systemic risks posed by gatekeepers. This instrument seeks to prevent, rather than merely remedy, exploitative or exclusionary conduct. Crucially, the DMA addresses certain shortcomings of the GDPR by explicitly prohibiting the combination of personal data across services without valid user consent and mandating interoperability, data access, and platform neutrality. These obligations function independently of the GDPR, but they also reinforce its goals by embedding structural guarantees that pre-empt coercive data practices.

2. Consent under the DMA and Its Impact on the GDPR Legal Framework

The Digital Markets Act introduces a paradigm shift in regulating dominant digital platforms by imposing *ex ante* obligations on so-called *gatekeepers*. According to Article 3(1) DMA, a gatekeeper is an undertaking that provides a core platform service and (a) has a significant impact on the internal market, (b) operates a core platform service which serves as an important gateway for business users to reach end users, and (c) enjoys an entrenched and durable position in its operations—or is

danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Komentarz in *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, ed. Paweł Litwiński, 1st ed. (Wydawnictwo C.H. Beck, 2021).

[9] Judgment of the Court of Justice of the European Union of 4 July 2023, *Bundeskartellamt v. Meta* (C-252/21), ECLI:EU:C:2023:537.

foreseeably acquiring such a position. The designation procedure under Article 3(4) further empowers the European Commission to formally list undertakings as gatekeepers, based on qualitative and quantitative criteria, creating a clearly defined regulatory perimeter.

Once designated, gatekeepers are subject to a set of obligations outlined in Articles 5, 6, and 7 DMA. Among these, Article 5(2) plays a critical role in the data governance framework, as it introduces a substantive limitation on how gatekeepers may process personal data. It provides that a gatekeeper shall not: "without complying with the relevant provisions of Regulation (EU) 2016/679: (a) process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core platform services of the gatekeeper; (b) combine personal data from the relevant core platform service with personal data from any other core platform services or from any other services provided by the gatekeeper or with personal data from third-party services; (c) cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services; and (d) sign in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and has given consent in the sense of Article 4(11) and of Article 7 of Regulation (EU) 2016/679."

This cross-reference to the GDPR has a profound legal effect. It imports into the DMA context the high threshold for valid consent developed under Articles 4(11), 6(1)(a), and 7 GDPR, but operationalises it in a structurally different regime. Unlike the GDPR, where consent is merely one of six equally valid legal bases for processing under Article 6(1), the DMA effectively eliminates alternative grounds, such as contract performance or legitimate interest, in the specific scenario of combining personal data across services.

In the case of contractual necessity (Art. 6(1)(b) GDPR), processing must be genuinely necessary to fulfil the contract's core service. Common breaches are related to asserting that extensive profiling or targeted ads are "essential" for a platform's primary service (despite EDPB guidance that truly "necessary" means it cannot function without such processing) or combining user data from multiple services. In *Bundeskartellamt v. Meta*, the court emphasized that "needing" data for customized features does not automatically make it "necessary" for basic service functionality.[10] EDPB repeatedly underscores a narrow interpretation of "necessary." Customization or targeted advertising is typically not deemed inherently necessary for providing the core functionality of a service.

Moreover, when it comes to legitimate interest (Art. 6(1)(f) GDPR), the controller's interest must be balanced against the data subject's rights and freedoms. Common breaches include treating revenue-driven advertising interests as auto-

[10] Judgment of the Court of Justice of the European Union of 4 July 2023, *Bundeskartellamt v. Meta*.

matically "legitimate" or failing to offer meaningful opt-outs that would allow users to avoid invasive tracking or profiling. EDPB guidelines and CJEU rulings highlight that balancing must account for the platform's market power and user vulnerability; a gatekeeper's interest in personalized ads does not necessarily override user privacy rights.

Consequently, DMA effectively narrows the scope of legal grounds for data processing by introducing stricter conditions. The EDPB has highlighted this limitation in its Opinion 08/2024, emphasizing that gatekeepers must not use their dominant position to nudge users into providing consent under pressure or as a precondition for accessing the service.[11]

In other words, gatekeepers cannot rely on other legal bases from Article 6 GDPR to justify cross-service data processing—even where such justifications might otherwise be permissible under the GDPR. This approach constitutes a deliberate legislative recalibration. By embedding a strict consent requirement directly into competition regulation, the DMA aims to prevent gatekeepers from leveraging their ecosystem power to circumvent user autonomy through contract or default design choices. It explicitly precludes common strategies such as bundling consent with terms of service or invoking legitimate interest for behavioural profiling—tactics frequently employed to sidestep the high bar for GDPR-compliant consent.

Moreover, the DMA requires that such consent be "freely given, specific, informed and unambiguous," echoing the language and interpretative standards from the GDPR, including those elaborated in the *Planet49* ruling and EDPB Guidelines. Furthermore, gatekeepers are prohibited from using so-called "consent or pay" models without offering a genuinely equivalent no-cost alternative, particularly where the service is otherwise offered free of charge.[12] This interpretation, though not explicitly found in the text of the DMA, stems from recent enforcement actions, including the European Commission's April 2025 decision addressing Meta's use of such models.[13] In that decision, the Commission found that users were not given a real choice and that consent was not freely given, thereby breaching both GDPR standards and DMA obligations.

The two regimes operate in a complementary but asymmetric manner. While the GDPR governs the processing of personal data generally, the DMA constrains the structural preconditions under which certain processing is allowed, targeting systemic behaviours rather than isolated infractions. This differentiation responds to

[11] European Data Protection Board, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, adopted on 17 April 2024, available at: https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf , accessed 5 July 2025.

[12] Klaudia Majcher, "Freedom, Power, and Contestability: Interactions between Article 5(2) DMA and the GDPR," Kluwer Competition Law Blog, published 22 October 2024, https://legalblogs.wolterskluwer.com/competition-blog/freedom-power-and-contestability-interactions-between-article-52-dma-and-the-gdpr/.

[13] European Commission, *Decision on Meta's Consent Model*, published 23 April 2025, https://digital-markets-act.ec.europa.eu/commission-finds-apple-and-meta-breach-digital-markets-act-2025-04-23_en.

the specific challenges posed by digital conglomerates, whose ability to accumulate and repurpose user data at scale cannot be adequately addressed by the reactive enforcement model of the GDPR alone.

3. Enforcement Challenges and Institutional Division of Competences

While the elevation of consent as a cornerstone of lawful data processing under both the GDPR and the DMA appears, in principle, to empower data subjects, the increasing reliance on consent also presents significant challenges. Scholars have argued that an overemphasis on consent risks creating a compliance burden that paradoxically undermines user autonomy. As Ella Corren points out, the proliferation of consent requests may lead to "consent fatigue," rendering individuals less capable of making meaningful choices and more likely to accept intrusive processing by default.[14] This critique suggests that the strengthening of consent mechanisms does not automatically translate into stronger data protection, especially when power asymmetries between users and gatekeepers persist.

These difficulties are further compounded by the structural divergence in enforcement mechanisms under the GDPR and the DMA. The GDPR is enforced primarily by national data protection authorities (DPAs), coordinated through the European Data Protection Board (EDPB), with a significant role played by lead supervisory authorities under the so-called one-stop-shop mechanism. By contrast, enforcement of the DMA is centralized in the hands of the European Commission, which acts as the sole enforcer. This institutional asymmetry creates potential tensions: while the GDPR leaves room for diverse national interpretations and enforcement approaches, the DMA pursues uniform application by design.[15]

Moreover, the enforcement competences of the Commission under the DMA extend to practices that also fall within the remit of data protection law. Article 5(2) DMA, as previously discussed, prohibits certain types of personal data processing unless based on GDPR-standard consent. However, it is the Commission—not the DPAs—that enforces this prohibition. This dual structure raises open questions about fragmentation, duplication of proceedings, and the risk of conflicting interpretations regarding what constitutes valid consent. While coordination

[14] Ella Corren, "The Consent Burden in Consumer and Digital Markets," *Harvard Journal of Law & Technology* 36, no. 2 (2023): 551.

[15] Iga Małobęcka-Szwast, "Commentary on Article 5," in *Akt o rynkach cyfrowych—Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828. Komentarz* in *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, ed. Mateusz Grochowski, 1st ed. (Wydawnictwo C.H. Beck, 2024).

mechanisms may be developed in the future, the current regulatory framework lacks a formalized process for resolving such overlaps between the data protection and competition regimes.

In response to the DMA's constraints, some gatekeepers may restructure their offerings to separate essential from non-essential processing activities, thereby reducing reliance on personal data for ad-targeting or cross-service analytics. The GDPR principle of data minimization resonates with the DMA's insistence on functional user alternatives that do not rely on exhaustive data collection.[16] Platforms might, for instance, develop "light" service versions with minimal data usage to enable a genuine choice for users who opt out of more invasive practices.

Debates persist regarding whether gatekeepers can lawfully require payment from users who decline data-intensive processing. The DMA suggests that simply imposing a fee on non-consenting users may be impermissible if it effectively nullifies the freedom to say no. Any such model would be subject to scrutiny under Article 5 of the DMA, particularly if a free version of the service exists or if the pay-only alternative appears punitive. As enforcement agencies clarify the regulatory landscape, it remains to be seen whether certain "consent or pay" options will survive under the dual GDPR–DMA regime.

In essence, the DMA amplifies the GDPR principle of free and informed user decision-making by prohibiting gatekeepers from relying on weaker or overbroad legal bases for data processing, such as legitimate interest or contractual necessity, when delivering key platform services. This dual framework fosters greater user autonomy and curtails exploitative data practices. Gatekeepers can no longer simply rely on fallback justifications; they need valid, uncoerced consent.

Although the GDPR and the DMA are grounded in different legal spheres, they converge on a shared objective of ensuring genuine user autonomy. The GDPR seeks to protect fundamental rights by demanding a robust legal basis for data processing, while the DMA aims to preserve market contestability by preventing gatekeepers from leveraging their dominance to coerce consent. This synergy is reflected in the stringent conditions the DMA imposes on gatekeepers, effectively reinforcing the GDPR's emphasis on freely given, informed, and specific user consent.

The European Data Protection Board and the European Commission have announced plans to coordinate on issues at the intersection of the GDPR and DMA, an initiative likely to yield more detailed guidance on how gatekeepers should reconcile data protection obligations with competition-based restrictions.[17] Future case law, enforcement decisions, and interpretive documents will further clarify how these

[16] Hatim Rahman et al., "Taming Platform Power: Taking Accountability into Account in the Management of Platforms," *Academy of Management Annals* 18, 1 (2025): 251–94, https://doi.org/10.5465/annals.2022.0090.

[17] European Data Protection Board, *EDPB to Work Together with the European Commission to Develop Guidance on the Interplay of the GDPR and the DMA*, 2024.

two regulatory frameworks should be applied, particularly in complex scenarios involving multi-service integration and targeted advertising at scale.

Through Article 5 of the DMA, EU law now exerts a direct influence over which GDPR legal grounds can be legitimately cited by gatekeepers. The result is a narrower scope for contractual necessity and legitimate interest, with corresponding emphasis on uncoerced user consent. In this manner, the DMA both reinforces and extends GDPR principles by insisting on robust user autonomy, enhanced accountability for dominant platforms, and the prohibition of exploitative data practices. The evolution of EU law thus illustrates how data protection and the DMA's *ex ante* rules increasingly function as complementary tools to address the challenges of pervasive data-driven business models. Dominant platforms must recognise that genuine user freedom is not merely an aspiration within the GDPR; under the DMA, it has become a firm legal requirement with tangible market and enforcement implications.

Summary

The European Union's regulatory response to the rapidly evolving digital ecosystem reflects both the ambition and the difficulty of legislating in a space where technological innovation consistently outpaces legal adaptation. While the General Data Protection Regulation laid the foundation for a fundamental rights-based approach to personal data processing, the Digital Markets Act introduces a complementary *ex ante* instrument that directly targets the structural imbalances in platform-dominated markets. The effectiveness of this dual framework now hinges on the European Commission's enforcement strategy.

This article has demonstrated that although the DMA is formally distinct from the GDPR, it places substantial constraints on the data processing practices of gatekeepers by limiting their reliance on weaker legal bases such as legitimate interest or contractual necessity. By mandating real, unbundled user choice, the DMA effectively elevates the standard for valid consent in contexts where market dominance might otherwise undermine voluntariness.

Recent developments confirm this regulatory trajectory. The EDPB's Opinion 08/2024 and the European Commission's decision concerning Meta's "consent or pay" model exemplify a growing synergy between data protection and digital market regulation. These developments suggest a strategic shift from purely parallel enforcement to a more integrated regulatory philosophy—one that embeds data protection concerns directly into competition-driven obligations.

Notably, the DMA departs from the GDPR's decentralised enforcement model by granting the European Commission exclusive competence to monitor and sanction gatekeeper conduct. This centralisation aims to ensure coherence and efficiency in

enforcement, yet it also introduces challenges related to institutional coordination and potential regulatory fragmentation. The interplay between the GDPR, national DPAs, and the Commission under the DMA thus raises important normative and practical questions, particularly concerning the consistency of standards, the risk of overlapping obligations, and the allocation of investigative authority. As enforcement practice evolves, the Union's capacity to reconcile its dual commitment to fundamental rights and fair markets will be increasingly tested.

In this sense, the GDPR provides the normative grammar for lawful data processing, whereas the DMA imposes a structural syntax that reshapes how gatekeepers must operationalize consent, transparency, and accountability. Together, these regimes not only reinforce one another but also articulate a broader vision of user empowerment in the digital age. By aligning fundamental rights protection with market fairness, the EU aspires to re-balance the asymmetrical power relationship between dominant platforms and individual users—an endeavour whose success will ultimately depend on coherent, robust, and forward-looking enforcement.

BIBLIOGRAPHY

Barta, Paweł, Maciej Kawecki, and Paweł Litwiński. "Commentary on Article 6." In *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Komentarz* in *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, edited by Paweł Litwiński, 1st ed. Wydawnictwo C.H. Beck, 2021.

Corren, Ella. "The Consent Burden in Consumer and Digital Markets." *Harvard Journal of Law & Technology* 36, no. 2 (2023): 551–613.

Majcher, Klaudia. "Freedom, Power, and Contestability: Interactions between Article 5(2) DMA and the GDPR." Kluwer Competition Law Blog, published 22 October 2024. https://legalblogs.wolterskluwer.com/competition-blog/freedom-power-and-contestability-interactions-between-article-52-dma-and-the-gdpr/.

Małobęcka-Szwast, Iga. "Commentary on Article 5." In *Akt o rynkach cyfrowych—Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828. Komentarz* in *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, edited by Mateusz Grochowski, 1st ed. Wydawnictwo C.H. Beck, 2024.

Rahman, Hatim A., Arvind Karunakaran, and Lindsey D. Cameron. "Taming Platform Power: Taking Accountability into Account in the Management of Platforms." *Academy of Management Annals* 18, 1 (2025): 251–94. https://doi.org/10.5465/annals.2022.0090.

Wójtowicz, Aleksandra. "U.S. and EU Clash over Regulation of Digital Content Moderation." Polski Instytut Spraw Międzynarodowych, published 21 March 2025. https://pism.pl/publications/us-and-eu-clash-over-regulation-of-digital-content-moderation.

ZESZYT PRAWNICZY UAM
NR 15/2025
https://doi.org/10.14746/zpuam.2025.15.10

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

JOLANTA ŻÓŁKIEWSKA

Adam Mickiewicz University, Poznań, Poland
https://orcid.org/0000-0002-8741-4243
jolzol@st.amu.edu.pl

Proceedings for the Imposition of Administrative Fines

Abstract: The purpose of this article is to present selected proceedings for the imposition of administrative fines. In the Polish legal system, there are provisions on the subject in the Administrative Procedure Code, but there are also a number of separate special provisions in selected areas of law in which it happens that selected provisions of Section IVa of the Administrative Procedure Code do not apply. This paper presents the proceedings of administrative fines in areas of law such as protection of historical monuments, GDPR, higher education and science and environmental protection. Drawing attention to the multiplicity of regulations on administrative fines is extremely important to increase legal awareness.

Keywords: administrative fines, protection of monuments, higher education and science, environmental protection, GDPR

Introduction

Administrative monetary penalties, although they have been functioning in the Polish legal system for several decades, their definition appeared relatively recently, as only in the 2017 amendment to the Code of Administrative Procedure—Act of 7 April 2017 amending the Act—Code of Administrative Procedure and certain other acts, which entered into force on 1 June 2017[1] and introduced a number of provisions concerning it. Provisions on administrative fines are included not only in this Act, but in a number of legal acts from various fields, such as the law on environmental protection, protection of personal data or monuments. This article presents the results of an analysis of the legal provisions on administrative fines in each area of law.

1. The Essence of an Administrative Fine

Introduced in Article 189b of the Act of 14 June 1960, the Code of Administrative Procedure,[2] the concept of an administrative fine has not changed and is currently understood as 'a pecuniary sanction specified by law, imposed by a public administration authority, by way of a decision, following a breach of law involving

[1] Ustawa z dnia 14 czerwca 1960 r.—Kodeks postępowania administracyjnego (consolidated text Journal of Laws of 2017, item 1257 as amended).

[2] Ustawa z dnia 14 czerwca 1960 r.—Kodeks postępowania administracyjnego (consolidated text Journal of Laws of 2024, item 572 as amended), hereinafter: k.p.a.

non-compliance with an obligation or prohibition imposed on a natural person, legal person or organisational unit without legal personality'. An administrative pecuniary penalty is therefore the negative consequence of a failure to comply with a legal order or prohibition of the addressee, which consists in the use of coercion, being an element of state authority.[3] It is an ailment imposed for the violation of a legal norm without taking into account the fault of the offender. First and foremost, however, an administrative monetary penalty is a sanction of a pecuniary nature, which distinguishes it from an administrative fee, the incurrence of which is associated with the exercise of powers for which the law requires the payment of costs.[4]

Polish administrative law is characterised by the multiformity of administrative fines, which is related to the existing diversity of legal relations. This manifests itself, for example, in the nomenclature itself, since, in addition to the concept of 'administrative monetary penalty', the legal provisions of the Polish system also contain names such as 'financial penalty', 'sanction fee', 'increased fee' or 'additional tax liability'.[5] As to the essence of administrative fines, they are not fines according to criminal law, as the Constitutional Court has unequivocally stated.[6]

Administrative monetary penalties perform a variety of functions, of which, according to many positions, the main one is the preventive function, aimed primarily at 'deterring' actors from committing violations of the law, but also protecting the safety of people and property.[7]

An administrative monetary penalty is intended to encourage compliance with the legal order and to discourage future violations of certain obligations. For this reason, the preventive function is assumed to be their overriding objective, taking into account the second of the basic functions of an administrative fine, which is the repressive function.[8] Repression is already indicated by the very name 'punishment'. Here, repression does not mean retribution for the breach of a legal duty, but a coercive measure to ensure the fulfilment of the administration's tasks, as outlined by the Constitutional Court in its position paper.[9] Another of the functions performed by the administrative monetary penalty is the compensation function, or compensatory function, which consists in ordering the payment of a certain sum of money

[3] Dorota Fleszer, "Administracyjne kary pieniężne," *Roczniki Administracji i Prawa*, no. 1 (2022): 90–92.

[4] Barbara Adamiak, "Commentary on Article 189b," in Barbara Adamiak and Janusz Borkowski, *Kodeks postępowania administracyjnego: Komentarz 2024* (Legalis/el., 2024).

[5] Fleszer, "Administracyjne kary pieniężne," 92.

[6] Judgment of the Constitutional Tribunal of April 29, 1998, K 17/97, saos.org.pl.

[7] Helena Kisilowska and Grzegorz Zieliński, "Administracyjne kary pieniężne—funkcja prewencyjna i represyjna," *Prawo w działaniu. Sprawy karne*, no. 43 (2020): 165, https://doi.org/10.32041/pwd.4309.

[8] Fleszer, "Administracyjne kary pieniężne," 95.

[9] Judgment of the Constitutional Tribunal of March 31, 2008, SK 75/06, consolidated text Journal of Laws of 2008 No. 57, item 349 as amended.

for the damage related to the violation of a prohibition or the non-performance of an obligation imposed by law.[10]

The provisions of Section IVa of the Code of Civil Procedure, which provide for administrative fines, do not indicate the procedure to be followed in cases involving them, nor do they refer to the norms of the Criminal Code[11] or the Code of Criminal Procedure.[12] According to the assumption of the Code of Administrative Procedure Act, administrative pecuniary penalties concern only administrative law and, in accordance with its provisions and rules, they are imposed and imposed, and consequently the institutions authorised to carry out said actions are the competent public administration bodies. An administrative monetary penalty is imposed on an entity by means of an administrative decision. The provisions of the Code of Administrative Procedure, specifically Article 189d, only indicate the prerequisites for the imposition of administrative fines, which include the gravity and circumstances of the violation of the law, the subject's conduct, previous punishment, the degree of the party's contribution, the party's conduct, the consequences of the violation, and personal circumstances. The first prerequisite mainly includes the need to protect life or health, property of significant size, and 'important public interest or exceptionally important interest of the party', as well as the duration of the violation. The catalogue of enumerated values is not closed, and the enumeration itself includes the values included in the Constitution of the Republic of Poland. On the other hand, the manner of conduct of an entity means the frequency with which the entity has violated the same type of prohibitions or failed to comply with the same obligations in the past. When imposing a fine, the public administration body is obliged to take into account a previous punishment for the same offence or fiscal offence or misdemeanour. The degree of contribution of a party is related to the determination of whether the party acted with full knowledge and whether this was related to the actions of other persons. The offender's conduct relates to the circumstances of whether or not any action was taken to remedy the breach. The public administration body, as indicated above, also takes into account the fact of gaining or suffering a loss. The last-mentioned prerequisites, i.e. personal conditions, include, e.g. financial status, state of the family, living conditions of the family, state of health.[13]

---

[10] Marcin Gubała, "Administracyjne kary pieniężne w systemie szkolnictwa wyższego i nauki," *Ius Novum*, no. 3 (2022): 169, https://doi.org/10.26399/iusnovum.v16.3.2022.32/m.gubala.

[11] Ustawa z dnia 6 czerwca 1997 r.—Kodeks karny (consolidated text Journal of Laws of 2024, item 17 as amended).

[12] Ustawa z dnia 6 czerwca 1997 r.—Kodeks postępowania karnego (consolidated text Journal of Laws of 2025, item 46 as amended).

[13] Barbara Adamiak, "Commentary on Article 189d," in Adamiak and Borkowski, *Kodeks postępowania administracyjnego* (Legalis/el., 2024).

2. Proceedings for the Imposition of Administrative Fines in Monument Protection Law

The introduction of provisions on administrative fines into the Code of Administrative Procedure has contributed to the amendment of many other acts, one example of which is the Act on the protection and care of historical monuments. In this act, by virtue of the Act on amending the Act on the protection and care of historical monuments and some other acts,[14] Chapter 10A was introduced, which is entirely devoted to administrative monetary penalties and to which the provisions of the Code of Civil Procedure also apply. The provisions replaced the previous certain offences which had a criminal nature.[15] Administrative fines in the Act on the protection and care of historical monuments are imposed for certain types of violations, which are divided by the Act into failure to notify (Article 107a(1)), expiry of the permit (Article 107b(1)), obstructing access to the monument (Article 107c(1)), acting without a permit (Article 107d) and failure to implement post-inspection recommendations (Article 107e). The range of fines, depending on the type of act or omission, varies from PLN 500 to as much as PLN 500,000.[16] The aims of introducing the above regulations were, inter alia, to improve the protection of historical monuments in Poland and to counteract the legal instruments that have so far been ineffective in protecting them. Due to the discontinuation of criminal proceedings by the police and court rulings that were disproportionate to the degree of guilt, the criminal sanctions applied were not sufficiently effective to stop, for example, the destruction or damage of monuments, which also negatively affects the education of the public as to the proper handling of monuments.[17]

The imposition of administrative fines for the protection of monuments in practice is not consistent on a national scale, if only taking into account the structure and organisation of provincial offices for the protection of monuments, only some of which have separate departments or positions whose competences include conducting proceedings for the imposition of administrative fines. The author of one of the studies argues that due to the necessity of knowledge of separate regulations, jurisprudence or literature, conducting proceedings in this matter should be entrusted to an employee with an education in law, while the contribution of substantive employees should consist in collecting evidence that will enable proceedings to be initiated. The Act on the protection and care of historical mon-

[14] Ustawa z dnia 22 czerwca 2017 r. o zmianie ustawy o ochronie zabytków i opiece nad zabytkami oraz niektórych innych ustaw (consolidated text Journal of Laws of 2017, item 1595 as amended).

[15] Anna Michalak, "Administracyjne kary pieniężne w polskim prawie ochrony zabytków—kilka uwag o efektywności regulacji po czterech latach obowiązywania," *Przegląd Legislacyjny*, no. 1 (2022): 86.

[16] Ustawa z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami (consolidated text Journal of Laws of 2024, item 1292 as amended).

[17] Michalak, "Administracyjne kary pieniężne w polskim prawie ochrony zabytków," 88.

uments also contains legal loopholes, which result in the authority competent to impose a fine for the protection of historical monuments not having a legal basis for imposing the fine in the case of, for example, a situation in which the investor, despite the obligation under the construction permit, has not carried out archaeological research.[18]

Proceedings for imposing administrative fines for the protection of historic monuments conducted by Provincial Monument Conservators are often discontinued due to the disproportionality of staff involvement and financial outlay to the amount of the fine to be imposed, for example. The effectiveness of the administrative penalties introduced is therefore negligible and does not contribute to improving the state of monument protection in Poland.[19]

3. Proceedings for the Imposition of Administrative Fines in the Higher Education and Science System

The basic legal act of the higher education and science system is the Act of 20 July 2018—Law on higher education and science,[20] whose contents include regulations defining sanctions in the form of administrative fines for the breach of selected obligations set out in this Act. The imposition of administrative fines in this area is an action constituting a measure of supervision over the entities comprising higher education. According to Article 7(1) p.w.s.n., these entities of the higher education system include: (1) higher education institutions (HEIs); (2) federations of entities of the higher education and science system; (3) the Polish Academy of Sciences; (4) scientific institutes of the Polish Academy of Sciences; (5) research institutes; (6) international scientific institutes established on the basis of separate acts operating in the territory of the Republic of Poland; (7) the Łukasiewicz Centre; (8) institutes operating within the Łukasiewicz Research Network; (9) the Polish Academy of Arts and Sciences and (10) other entities conducting mainly scientific activity in an independent and continuous manner. These very entities, according to Article 426 p.w.s.n., are supervised by the minister responsible for higher education and science. However, administrative fines may only be imposed on legal entities, which do not include 'other entities that primarily carry out scientific activities in an independent and continuous manner', which are specific 'organisational and legal forms used to undertake these scientific and teaching activities'.[21] The purpose

[18] Michalak, "Administracyjne kary pieniężne w polskim prawie ochrony zabytków," 89–90.

[19] Michalak, "Administracyjne kary pieniężne w polskim prawie ochrony zabytków," 96–97.

[20] Ustawa z dnia 20 lipca 2018 r.—Prawo o szkolnictwie wyższym i nauce (consolidated text Journal of Laws of 2024, item 1571 as amended), hereinafter: p.w.s.n.

[21] Gubała, "Administracyjne kary pieniężne w systemie szkolnictwa wyższego i nauki," 174.

of administrative fines in the higher education and science system is to strengthen safeguards for the proper functioning of the system.[22]

Unlike the Act on the protection and care of historical monuments, the p.w.s.n. does not contain a separate section on administrative monetary penalties, and they are scattered in various sections of the act, often also as another of the paragraphs relating to a particular article. The provisions clearly indicate which entities can be fined. For example, while the addressees of Article 431 p.s.w.n. are HEIs, not every HEI has the right to impose an administrative fine on the Minister.[23] This is because two categories of HEIs are excluded from the minister's supervision: the majority of HEIs and higher seminaries run by churches and other religious associations, and some foreign HEIs and their branches. Another issue is the notion of 'minister' in the above article: as far as the interpretation of this particular provision is concerned, a minister is not only the minister responsible for higher education and science. In this case, the catalogue of bodies that supervise higher education institutions is broader. Indeed, this supervision may be exercised by other ministers, such as the minister responsible for military higher education institutions, the minister responsible for state service higher education institutions, the minister responsible for medical higher education institutions, the minister responsible for higher education institutions for maritime studies or the minister responsible for higher education institutions for art studies.[24]

Other entities in the higher education system subject to administrative fines are federations. According to Article 165 of the p.w.s.n., in order to fulfil their tasks jointly, these federations are formed by pairings of a public academic university with another public academic university, a research institute, an institute of the Polish Academy of Sciences or an international institute or a non-public academic university with another non-public academic university.

Both Article 175 p.w.s.n. and Article 431 p.w.s.n. indicate an extensive range of acts for which an administrative fine may be imposed, which the legislator has indicated by reference to other provisions. However, there are no regulations which would provide guidelines as to the assessment of the legitimacy or unjustifiability of the imposition of the penalty when the competent minister issues a decision. On the other hand, a gradation of infringements of the law has been introduced, which manifests itself in different amounts of fines, i.e. up to PLN 100,000, up to PLN 50,000, and up to PLN 5,000. The fine is imposed here is done so in a discretionary manner. As for the form of imposing the penalty, the provisions of the p.w.s.n. do not explicitly

[22] Gubała, "Administracyjne kary pieniężne w systemie szkolnictwa wyższego i nauki," 171.

[23] Gubała, "Administracyjne kary pieniężne w systemie szkolnictwa wyższego i nauki," 175.

[24] Piotr Rączka and Dominika Zawacka-Klonowska, "Administracyjne kary pieniężne jako forma nadzoru nad systemem szkolnictwa wyższego i nauki," in *Administracja publiczna wobec procesów zmian w XXI wieku: Księga jubileuszowa Profesora Jerzego Korczaka,* ed. Piotr Lisowski (Wydawnictwo Uniwersytetu Wrocławskiego, E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa, 2024), 697.

indicate this; therefore the form of an administrative decision referred to in Article 189b of the Code of Administrative Procedure should be adopted.[25]

Furthermore, there are no norms relating to the procedure itself for imposing administrative fines in the higher education system. Therefore, the provisions of the Code of Administrative Procedure, which regulates the principles of imposing such penalties, are also taken into account in this case. Moreover, the p.s.w.n. Act does not specify the appeal bodies for the imposition of an administrative fine by the minister, but also does not specify whether a party may appeal against the decision. It is assumed that the only means that a party may use is an application to the Minister for reconsideration of the case, under Article 127 §3 of the Code of Administrative Procedure.[26]

4. Proceedings for the Imposition of Administrative Fines in Environmental Law

Another of the many branches of law in which the legislator introduces norms concerning administrative fines is environmental law. In Poland, the basic legal act of this field is the Act of 27 April 2001—Environmental Protection Law.[27]

In contrast to the p.w.s.n. Act discussed in Chapter 3, the Environmental Protection Law also contains, in some cases, norms concerning the course of proceedings for the imposition of fines. The introduced solutions are exceptions to the norm contained in Article 1(1) of the Code of Administrative Procedure, stating that this code 'normalizes the proceedings before public administration bodies in individual matters belonging to the competence of these bodies and decided by administrative decisions or settled tacitly' and, according to the principle lex specialis derogat legi generali, the specific provision then excludes the validity of the general provision. One such provision, which indicates an exception, is Article 300(4) p.o.ś. This modifies Article 107 §1 of the Code of Administrative Procedure and thus indicates the elements that an administrative decision should contain.[28]

Monetary penalties in environmental law have various forms, as there are both relatively and absolutely marked penalties. Article 236d(1)(2) of the Environmental Protection Law may be used as an example of a peremptory penalty, which specifies

[25] Rączka and Zawacka-Klonowska, "Administracyjne kary pieniężne jako forma nadzoru nad systemem szkolnictwa wyższego i nauki," 698.

[26] Gubała, "Administracyjne kary pieniężne w systemie szkolnictwa wyższego i nauki," 183–84.

[27] Ustawa z dnia 27 kwietnia 2001 r.—Prawo ochrony środowiska (consolidated text Journal of Laws of 2024, item 54 as amended), hereinafter: p.o.ś.

[28] Krzysztof Gruszecki, "Postępowanie w przedmiocie wymierzania kar pieniężnych na podstawie Prawa ochrony środowiska—wybrane uwagi," *Prawne Problemy Górnictwa i Ochrony Środowiska*, no. 1 (2022): 19, https://doi.org/10.31261/PPGOS.2022.01.04.

that a penalty of PLN 5,000 is imposed in the event of failure to comply with certain obligations. Paragraph 2 of the same article also contains an example of a relative penalty of PLN 500 to PLN 25,000 in the event that the operator of an installation fails to ensure the quality of transmitted data. The aforementioned penalties are imposed by the provincial environmental protection inspector on the operator of the installation.

For some of the penalties contained in the p.o.ś., the legislator has specified the manner of determining the amount of these penalties. Moreover, a catalogue of acts for which the penalty may be incurred has been unambiguously indicated, i.e. in accordance with Article 273 of the p.o.ś. for exceeding or breaching the conditions of using the environment, established by a decision with respect to the introduction of gases or dust into the air, the issuance of an authorisation to emit greenhouse gases or the storage of waste, as well as with respect to the storage and emission of noise into the environment. In this respect, another of the provisions of the p.o.ś. clearly defines what the level of administrative fines depends on. Article 274 p.o.ś. measures the volume and type of gases or dust discharged into the air, the amount and type of waste stored or stored and the time of storage or warehousing or the time of day and the size of the excess of the permissible noise level.

The entities that are obliged to bear the aforementioned penalties are entities using the environment (Article 275 p.o.ś.). In contrast to the examples of administrative fines described in Chapter 2 (the Act on the Protection and Care of Monuments), and Chapter 3 (the Act on the Law on Higher Education and Science), environmental law is more comprehensively regulated. Specifically, the legislator has regulated the grounds for initiating proceedings on this subject in Article 273 p.o.ś., i.e. initiation ex officio or at the request of the entity using the environment, which is subject to the fee or penalty (Article 282 p.o.ś.); the authority into whose account the imposed penalty should be paid (according to Article 277(3), this is the provincial environmental protection inspector who issued the decision on imposing the penalty); and the entities which derive income from the proceeds of the penalties (Article 272(4) p.o.ś.). Here, the monies obtained from penalties do not constitute revenue for the provincial environmental protection inspector, but for the National Fund for Environmental Protection and Water Management, provincial funds for environmental protection and water management, as well as for districts and municipalities.

The regulations determining the procedure for imposing administrative fines in environmental law have been introduced in a separate section, which can be found further down in the legislation. This section also specifies the following details regarding administrative fines: catalogue of offences for which an administrative fine is imposed (Article 298 p.o.ś.); the basis for ascertaining them, which, pursuant to Article 299 p.o.ś., are inspections and measurements carried out by the entity using the environment; the amount of the fine itself. Here, attention should be drawn to the manner of imposing penalties, since, as a rule, a fine is imposed at a level 20 times the unit rate of fees for introducing gases or dust into the air

(Article 309(1) p.o.ś.), while, for example, the upper unit rate of the penalty for exceeding the permissible level of noise penetrating into the environment is PLN 48 per 1 dB of exceedance (Article 311(1) p.o.ś.). The legislator in Article 308 p.o.ś. has also introduced a minimum sample from which proceedings on the imposition of a fine are initiated. Pursuant to this, entities are exempted from incurring fines if the anticipated amount of the fine does not exceed PLN 800. The Environmental Protection Law also contains regulations on fines for the failure to prepare and implement air protection programmes and short-term action plans. The fines that may be incurred by the responsible authorities here are relatively more, ranging from PLN 50,000 to PLN 500,000. They are issued by way of a decision, against which an appeal is expressly indicated. It indicates the competent authority (Article 315g p.o.ś.).

5. Proceedings for the Imposition of Administrative Fines for Violations of Personal Data Protection

The next most recent example of the introduction of administrative fines into a specific, detailed legal regime of a given branch of law is the inclusion of provisions on administrative fines for violations of personal data protection in various pieces of legislation, both national and EU. The main piece of legislation talking about this is 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.[29] The second act is the Data Protection Act of 10 May 2018.[30] In Polish legislation, prior to the entry into force of the Personal Data Protection Act, there were no administrative fines for personal data breaches, but only criminal provisions and sanctions in the form of a fine, restriction of freedom or imprisonment.[31] Currently, the law contains an entire chapter dedicated to penalties, i.e. Chapter 11 'Provisions on administrative fines and criminal provisions', which contains 8 articles (from 101 to 108), including 6 on administrative fines and 2 on criminal liability. However, the basic sanctions for personal data violations are strictly administrative fines. The scope of these administrative fines in the Law of 10 May 2018 does not go beyond that indicated in the GDPR, whose provisions are consistent across the European Union and provide a guarantee of effective protection of the rights of the.[32]

[29] 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) (OJ L 119, 4.5.2016, pp. 1–88).

[30] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (consolidated text Journal of Laws of 2019, item 1781 as amended).

[31] Art. 36, Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

[32] Art. 37 and 39, Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

Pursuant to the provisions of the Personal Data Protection Act, specifically Article 101, the supervisory authority which is authorised in Poland to impose administrative fines in this respect is the President of the Office for Personal Data Protection (PUODO). The provision also specifies the form of imposing penalties, which is a decision, as well as the group of privileged entities as regards being subject to penalties. Pursuant to the above article, the PUODO may impose a penalty on an entity obliged to comply with the provisions of GDPR, other than a public finance sector entity, a research institute and the National Bank of Poland. The penalty is imposed on non-privileged entities on the basis and conditions set out in Article 83 GDPR. The amount of these penalties, depending on the case, according to this article, reaches €10,000,000 and can sometimes even amount to €20,000,000. On the other hand, the maximum amount of penalties of units of the public finance sector, referred to in Article 9, points 1–12 and 14 of the Act of 27 August 2009 on public finance, research institutes and the National Bank of Poland is specified in Article 102 of the Act on personal data protection and amounts to PLN 100,000. Units of the public finance sector include public authorities, local government units, public universities, budgetary units or executive agencies. In the case of state and local government cultural institutions, the Act sets the maximum administrative fine at PLN 10,000.

In order to determine the amount of the administrative penalty on the entity obliged to comply with the provisions of the GDPR, the President of the Office for Personal Data Protection, pursuant to Article 101a of the Personal Data Protection Act, may request from the entity, and the entity is obliged to provide the PUODO, with the necessary data within 30 days of receiving the request. However, if the entity fails to provide the data needed to determine the basis of the penalty assessment, the PUODO shall determine the basis of the assessment in an estimated manner, taking into account the size of the entity, the specific nature of its business or the entity's general financial data.

The provisions of Article 189d–189f and Article 189k of the Code of Civil Procedure shall not apply to the imposition of administrative fines for personal data breaches. Therefore, in addition to the Act on the Protection of Personal Data, the other provisions of the Code of Civil Procedure shall apply. The decision on the administrative fine is an administrative decision which, pursuant to Article 105 of the Act on the Protection of Personal Data, shall be paid within 14 days from the expiry of the time limit for filing a complaint, or from the date on which the decision of the administrative court becomes final. At the request of the subject, the PUODO may postpone this deadline or divide the administrative penalty into instalments. However, interest is charged in both cases.

Regulations on the imposition of administrative fines for personal data violations are not dead laws, as evidenced by numerous decisions issued by PUODO. The level of administrative fines actually imposed is not low. For example, by decision

DKN.5131.1.2025[33] a fine of PLN 100,000 was imposed on the Ministry of Digitization, and a fine of PLN 27,124,816 was imposed on Poczta Polska S.A., or by decision DKN.5131.4.2024[34] one entity was charged with fines of PLN 687,534.75 and PLN 458,356.50. In 2024 alone, PUODO imposed administrative fines on 23 entities, which are collectively required to pay the sum of PLN 13,309,897.80.[35]

Summary

The regulations on administrative fines presented here indicate a multiplicity of differing provisions. In each of the selected areas of law, specific provisions have been introduced to achieve a specific, legitimate result. The differences appear not only in the procedural aspect. It is of particular importance to determine the amount of the penalty depending on the type of infringement. The wide range of these amounts should be noted here, as should the fact that, for the most part, the penalties are discretionary. The amount of the penalty is decided by the authority with the competence to impose administrative fines in the given scope. However, information on the actual administrative fine amounts applied in practice is not publicly available: only in the area of personal data violations does the PUODO publish its decisions, in which information on the amount of the penalty imposed for a given violation is public.

BIBLIOGRAPHY

Adamiak, Barbara. "Commentary on Article 189b." In Barbara Adamiak, Janusz Borkowski, *Kodeks postępowania administracyjnego: Komentarz 2024*. Legalis/el., 2024.

Adamiak, Barbara. "Commentary on Article 189d." In Barbara Adamiak, Janusz Borkowski, *Kodeks postępowania administracyjnego: Komentarz 2024*. Legalis/el., 2024.

Fleszer, Dorota. "Administracyjne kary pieniężne." *Roczniki Administracji i Prawa*, no. 1 (2022): 89–100.

Gruszecki, Krzysztof. "Postępowanie w przedmiocie wymierzania kar pieniężnych na podstawie Prawa ochrony środowiska—wybrane uwagi." *Prawne Problemy Górnictwa i Ochrony Środowiska*, no. 1 (2022): 1–19. https://doi.org/10.31261/PPGOS.2022.01.04.

Gubała, Marcin. "Administracyjne kary pieniężne w systemie szkolnictwa wyższego i nauki." *Ius Novum*, no. 3 (2022): 167–87. https://doi.org/10.26399/iusnovum.v16.3.2022.32/m.gubala.

Kisilowska, Helena, and Grzegorz Zieliński. "Administracyjne kary pieniężne—funkcja prewencyjna i represyjna." *Prawo w działaniu. Sprawy karne*, no. 43 (2020): 160–71. https://doi.org/10.32041/pwd.4309.

[33] PUODO decision of March 17, 2025, DKN.5131.1.2025.

[34] PUODO decision of January 17, 2025, DKN.5131.4.2024.

[35] Małgorzata Cwynar, "Kary finansowe za naruszenia RODO—podsumowanie roku 2024," Soczko & Partnerzy—Ochrona Danych, published 31 January 2025, https://www.soczko.pl/iod-soczko-partnerzy/blog-ochrona-danych/kary-finansowe-za-naruszenia-rodo-podsumowanie-roku-2024/.

Michalak, Anna. "Administracyjne kary pieniężne w polskim prawie ochrony zabytków—kilka uwag o efektywności regulacji po czterech latach obowiązywania." *Przegląd Legislacyjny*, no. 1 (2022): 78–98.

Rączka, Piotr, and Dominika Zawacka-Klonowska, "Administracyjne kary pieniężne jako forma nadzoru nad systemem szkolnictwa wyższego i nauki." In *Administracja publiczna wobec procesów zmian w XXI wieku: Księga jubileuszowa Profesora Jerzego Korczaka*, edited by Piotr Lisowski. Wydawnictwo Uniwersytetu Wrocławskiego, E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa, 2024.

ISSN (Online) 2956-2767
ISSN (Print) 2720-2526