*Teka Komisji Prawniczej PAN Oddział w Lublinie*
*vol. XVIII, 2025, no. 2, pp. 233–248*
https://doi.org/10.32084/tkp.9640

# ARTIFICIAL INTELLIGENCE IN THE PUBLIC SPHERE: LEGAL AND SECURITY CULTURE IN THE EU

Dr. habil. Marek Górka, University Professor

Koszalin University of Technology, Poland
e-mail: marek_gorka@wp.pl; https://orcid.org/0000-0002-6964-1581

**Abstract.** This article analyzes the impact of the development of artificial intelligence (AI) on the public sphere and its consequences for political, security, and legal culture. The paper describes how the advancement of AI forces a reinterpretation of existing legal, ethical, and philosophical assumptions. It focuses on the new European Union regulation concerning AI, which balances the need for innovation with the obligation to protect citizens' rights, highlighting AI's role in shaping international interactions and public policy. The article also addresses challenges related to disinformation, human rights, and the potential future risks associated with the use of AI.

**Keywords:** political culture; security culture; legal culture; artificial intelligence; digital law; EU security policy.

## INTRODUCTION

The analysis of the impact of artificial intelligence (AI) on the public sphere is currently a popular topic of many academic reflections and serves as a starting point for research on the extent to which the existing reality is changing [Radanliev 2025]. From the perspective of security itself, AI has a wide range of different applications. In today's reality, there are many automated programs that form the foundation of daily life, which, despite their beneficial applications, raise many questions about who makes decisions and on what basis [Pham and Davies 2024]. These types of questions simultaneously present challenges and expand research areas within legal culture regarding the regulation of algorithms, and in terms of decision-maker accountability for political culture, as well as in the context of protection against abuses and cyber threats for security culture. Of course, a natural question arises: in which direction is the development of artificial intelligence heading, and which entities and fields are driving it the most?

The potential implications of technological development are nothing new in the history of humanity; every change has brought the need to rethink existing philosophical, ethical, and legal assumptions. It has also forced

*ISSN 1899-7694*
*e-ISSN 2719-7379*

reinterpretations, sometimes even profound changes, in the political sphere, such as the invention of printing by Johannes Gutenberg in 1440, which led to, among other things, the Reformation. Almost six centuries later, the "digital revolution of print," including the widespread use of digital communicators, provided an impetus for many social and political movements and uprisings worldwide, such as the Arab Spring (2010-2012), the Black Lives Matter Movement (2013), and the Climate Strikes – Fridays for Future (2018). The dynamics of these transformations highlight the necessity to adapt legal culture to new challenges related to the regulation of digital content and the protection of civil rights, political culture to the growing role of social media in democratic processes, and security culture to the threats posed by disinformation, digital surveillance, and cyberattacks, which can destabilize social and political order.

Currently, revolutionary transformations are occurring in the way knowledge and information are perceived and managed. Knowledge, being a key resource in society, determines not only economic processes but also power structures, social relations, and legal systems. The greatest challenge is not the distant future dominated by advanced technologies, but the revolutionary changes that are already impacting everyday life [Hunter, Albert, Rutland, et al. 2024]. In Europe, where democracy and law have traditionally been seen as guarantees of freedom, there are increasing challenges related to the concentration of power. New centers of influence are emerging that go beyond traditional state structures. Power is increasingly intertwining, creating systems in which decisions are made based on data rather than democratic values or legal norms. Algorithms make decisions about granting loans, social benefits, or even job dismissals, often without transparent rules or the possibility of appeal [Purcell and Bonnefon 2023]. In this context, it is worth asking whether, alongside the changing surrounding reality, the nature of political culture, security culture, and legal culture, as well as the interrelationships between these areas, is also changing.

The content of the article aligns with the growing body of research on political, security, and legal cultures in the context of regulations concerning artificial intelligence. Among the key works in this field are: Christou, Meyer, and Fanni, who analyze the role of the European Union as a global leader in AI regulation [Christou, Meyer, and Fanni 2024], Bakiner, who examines pluralistic sociotechnical imaginaries in the context of the European Union's Artificial Intelligence Act [Bakiner 2023], and Kusche, who discusses the potential harms related to AI and their impact on fundamental rights and risk assessment [Kushe 2024].

The main objective of this paper is to characterize how AI is changing decision-making principles in the fields of politics, security, and law. The starting point here is to focus on the relationships between political culture, security culture, and legal culture, and their mutual influence in the context of AI. By doing so, the aim is to provide answers to the question of how priorities and values reflect the approach of law to new technologies and their implications for the future of democratic societies.

One of the main methods used in this paper is content analysis, which will be employed to identify the key fragments essential for the selected definitions of political, legal, and security culture. The next method is contextualization, which involves placing individual elements of these definitions within the context of technological development, with particular emphasis on the EU regulation on artificial intelligence,[1] in order to better understand the interrelationships between values in the areas of politics, law, and security, and the dynamic process of digitization. The third method used in this paper is the comparative method, which in this study involves comparing different definitions and approaches to culture, facilitating the identification of similarities and differences, as well as the evolution of these concepts in the context of the technological revolution driven by AI.

These research tools enable capturing the multifaceted nature of the subject matter, which also supports interdisciplinary understanding of phenomena at the intersection of technical and social sciences, which will certainly continue due to the increasing dominance of AI. The intention of reflecting on the impact of technology on political, security, and legal culture may bring a new perspective to the current discussion taking place in both academic and journalistic circles.

## 1. CONCEPTUALIZATION OF POLITICAL CULTURE, SECURITY CULTURE, AND LEGAL CULTURE

Culture is a broad conceptual collection, which means that in many definitions, certain aspects are more strongly emphasized or highlighted than others. This leads to the fact that individual descriptions of the term can be presented in different ways. However, a common denominator in most definitions of culture is its portrayal as the totality of humanity's achievements [Szymczak 1995, 1015; Polański 2008, 387; Dereń and Polański 2008; Olechnicki and Załęcki 1997, 106], encompassing both material and immaterial aspects [Szymczak 1995, 1015; Polański 2008, 387; Olechnicki and Załęcki 1997, 106-107; Dereń and Polański 2008], i.e., spiritual, intellectual, and social. Many definitions also point to the process of transmitting

[1] *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)* [hereinafter: Regulation 2024/1689], https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 [accessed: 30.03.2025].

culture [Szymczak 1995, 1015; Szymczak 2000; Olechnicki and Załęcki 1997, 106-107; Blackburn 2004] from one generation to the next, as well as its role in shaping the perception of the world and social norms.

Thus, in all the aforementioned works, culture is presented as a civilization achievement, inseparably accompanying humanity. It is also a constitutive factor of human existence, through the process of inheritance from generation to generation, where specific values are adopted, shaping the identity of society.

There are also differences in defining the concept of culture, which most often arise from the use of different approaches and semantic scopes. There are perspectives that view culture broadly, as the entire civilizational framework [Szymczak 2000], or as a spiritual or intellectual nature [Blackburn 2004]. Other differences exist between emphasizing the dynamic nature of culture, highlighting the transmission of values and norms [Olechnicki and Załęcki 1997, 106-107], and the static nature of culture as a collection of goods and achievements [Szymczak 2000]. Differences can also be observed by comparing definitions that, on one hand, equate culture with civilization as the technical development of society [Żmigrodzki 2003], and on the other, with a system of values and models.

The common elements, as well as the differences highlighted in many definitions, cause that selected fragments of the term "culture" can be assigned to the areas of political culture, security culture, or legal culture. Communities adopt cultural values and meanings to communicate and understand the environment along with its institutions that regulate social practices. In this context, another term arises: political culture, which is related to the assimilation of values and patterns recognized by a given community. However, it is not the collection of values that is important, but their hierarchy [Antoszewski and Herbut 1999, 260]. Not all communities, however, have the same forms of political culture. In the case of significant socio-political, religious, or historical contrasts, conflicts within a social group are often more pronounced. Therefore, it can be assumed that more homogeneous political cultures tend to have significantly greater stability.

Political culture refers to the ideas, beliefs, values, traditions, and practices that form the foundation of a political system [Olechnicki and Załęcki 1997, 107]. It is also a space of values that result from long-standing historical processes, as well as social, political, economic, and many other factors. Therefore, each state, in comparison to others, is characterized by its own, unique political culture [Walicka 2008, 279]. From this perspective, it is also easier to understand the causes of certain differences between individual states in areas such as political values, differing interpretations of human rights, or security policies.

The above statements – relating to political culture – highlight the interdependence and interaction between the cultural environment and the decision-making process. Political culture, therefore, represents the attitudes and orientations of members of a given society toward politics, which are composed of three factors: cognitive, affective, and evaluative. These include knowledge and interest in politics, the sense of influence and the degree of impact on political decisions, as well as the perceptions of the goals and functioning of the political system [Bankowicz 1999, 121; Antoszewski and Herbut 1999, 260].

The presence of elements such as attitudes, norms, and values in the descriptions of culture naturally leads to a correlation between them and social behaviors, particularly the level of civic engagement and awareness (Great Dictionary of the Polish Language). This, in turn, directly affects how citizens think about politics and indirectly influences the functioning of the state and its institutions [Olechnicki and Załęcki 1997, 106].

The second definitional area analyzed is security culture, the conceptualization of which also draws from broader cultural notions. A common element in both of these terms is certainly the factor that reinforces social and political experiences [ibid.]. Another important point is the repeated emphasis on the intergenerational transfer of knowledge, occurring both on an individual and institutional level [Szymczak 1995, 1015]. The concept of security culture has become a common term in the public sphere in recent years, undoubtedly due to numerous military and non-military events. Security culture focuses on aspects related to the protection of the state, society, and individuals from various threats [Misiuk, Itrich-Drabarek, and Dobrowolska-Opała 2021].

The third term is legal culture, whose definitions are also based on elements of the broader concept of culture. In this case, there are aspects that refer to norms and values related to adherence to the law [Olechnicki and Załęcki 1997, 106]. While this may not be a groundbreaking observation, it is important to note that law is most often derived from moral norms, which makes this factor correspond with the holistic view of culture.

Equally important elements of culture that form the foundations of law include intergenerational transmission, which in this case is seen as the process of legal education and socialization [Tokarczyk 2000, 61-64].

## 2. THE RELATIONSHIP BETWEEN POLITICAL CULTURE, SECURITY CULTURE, AND LEGAL CULTURE

Analyzing the definitional scope of these three cultures – political, security, and legal – it is clear that they are interconnected. To better understand the complexity of the nature of each of these cultures, it is essential to explore not only their changing nature due to digital progress but also their mutual influence on one another.

In this context, questions arise about the hierarchical and functional dependencies between these three concepts. In other words, which culture is dominant and encompasses a broad spectrum of norms, values, beliefs, and practices, and which one is a subset, thus focusing only on specific aspects related to a defined conceptual area? Another intriguing question that invites further consideration is which of these cultural categories determines and shapes the nature of the others?

According to many definitions, political culture plays a dominant role, as it encompasses the norms, values, and beliefs that shape the political system of a given society [Walicka 2008, 279]. It also defines the way power is exercised and the relationship between citizens and the state and its organs [Żmigrodzki and Sokół 1999, 165]. Assuming that politics forms the foundation of a state's functioning, it can be concluded that political culture has such a broad conceptual range that it includes both legal culture and security culture.

On the other hand, it must be noted that legal culture also shapes political culture. The values expressed in legal regulations indicate how citizens can or should perceive their duties in the public sphere. Therefore, a strong link exists between legal culture and political culture, leading to the conclusion that legal culture is an integral part of political culture.

On the other hand, law can be seen as a tool for implementing state policy. Specific provisions or regulations also reflect certain values, their hierarchy, and connections to selected areas of socio-political reality [Janowski 2012, 20-26]. Legal culture is conceptualized primarily in relation to society's relationship with the law. Therefore, it is assumed that many definitions emphasize knowledge, adherence to, and interpretation of the law in a social context [Chauvin, Stawecki, and Winczorek 2016, 45-47].

However, in terms of the mutual relationships between political and legal culture, it should be noted that any change in political culture, whether toward liberalism or authoritarianism, affects the shaping of legal culture. This, in turn, has a visible and often felt impact on civil rights or the functioning of the justice system.

Following this line of thought, a similar, analogous process can be observed, where political culture (shapes not only legal regulations) but also influences certain norms and principles in relation to security culture. In this context, it can be considered that security culture is a subset of state policy, as it involves actions related to protecting citizens, the state, and institutions from internal and external threats. At the same time, it largely relies on legal regulations, which provide the formal framework for its functioning. In summary, legal and political culture provide the foundations upon which the structure and direction of actions in the security sphere are built [Misiuk, Itrich-Drabarek, and Dobrowolska-Opała 2021, 128].

As we can see, the presented concept of the cultural triangle between the poles of politics, law, and security is complex and based on mutual interconnections. Political culture shapes the values and norms in society, which later contribute to the formation of the general security framework. In this regard, the model for the functioning of society and state institutions is shaped. This also influences the perception of actions aimed at ensuring a stable and predictable public space. Therefore, obligations, tasks, and rights regarding military and non-military threats are defined, creating the foundation for security culture.

## 3. AI REGULATION IN THE EUROPEAN UNION: BETWEEN POLITICAL CULTURE AND LEGAL CULTURE

In everyday life, various types of algorithms are used, ranging from large applications in industry or public spaces for facial recognition to smaller ones, such as those in smartphones for filtering spam in emails or personalizing content on social media. Artificial intelligence systems are also integral components of many physical products, such as toys, industrial machines, and medical devices. There is growing concern about the significant impact AI has on the health and safety of every user. A frequent public debate, which accompanies the introduction of new solutions and legal regulations – especially concerning new technologies – revolves around where the boundary should be drawn between innovation and the manner in which human rights or, alternatively, consumer protection in digital solutions will be ensured. This concern has become one of the primary reasons for the decision to regulate the functioning and application of the latest technologies in the public space, ensuring that they meet established safety standards [Crawford 2021, 45].

The EU Member States have approved an ambitious draft law regulating the use of artificial intelligence, which has been the subject of intense negotiations. The discussion on the legal boundaries of technology began in April 2021 when the European Commission, the administrative body of the European Union, introduced the legislative proposal.[2] By the end of 2022, the debate on the text became more urgent with the popularity of platforms such as ChatGPT.

This is the first framework regulation in the world to be established. The regulations are intended to ensure freedom and rights in the digital space. The ongoing discussion highlights that AI learns, evolves, and acquires

[2] *Proposal for a Regulation of the European Parliament and of the Council on Artificial Intelligence (Artificial Intelligence Act).* COM(2021) 206 final, April 21, 2021, https://ec.europa.eu/info/files/proposal-regulation-european-parliament-and-council-artificial-intelligence-act_en [accessed: 30.03.2025].

capabilities with unpredictable outcomes. So, does artificial intelligence develop faster than regulations? The problem is that the law can regulate technological phenomena, but the digital revolution occurs faster than the introduction of new norms that try to tame the pace of digital innovation.

An analysis of this document indicates that it consists of several key principles. The first concerns the protection of human rights, meaning that today, technology should indeed serve human rights, currently supporting democracy and ensuring that we all participate in the digital space (Regulation 2024/1689, pt. 48). The second principle is freedom of choice, allowing people to protect themselves from illegal or harmful content and ensuring that when using technologies like AI, they can do so safely (Regulation 2024/1689, pt. 53). The next principle is, of course, security – we are today accustomed to cyberattacks, but also to issues of solidarity and inclusion, as digital technology should serve to connect people, not divide them (Regulation 2024/1689, pt. 76). Participation aspects ensure that through digital technology, we can participate in democratic processes, and of course, sustainable development, as this digital transformation goes hand in hand with ecological transformation (Regulation 2024/1689, Article 59). This declaration effectively creates the foundation by combining what already exists, such as European data protection and privacy laws, while creating a framework for reference. This document represents how the European Union commits to a digital transformation that is sustainable, secure, citizen-focused, and, above all, reflects the values and fundamental rights that are the foundation of the EU. The principles provide full support for the development and implementation of AI in Europe, respecting European values while simultaneously safeguarding fundamental human rights, such as undisturbed privacy, transparency, and good social and ecological conditions. These regulations aim to limit risks and impose obligations on providers and those who create AI-based systems, depending on the level of risk they may pose [Christou, Meyer, and Fanni 2024, 383-401].

An important feature of the AI Act is its interoperability, which can be understood as a condition for the effective implementation and application of this document in practice. It cannot function in isolation from other legal regulations, nor can it be in conflict with them. The premise of this regulation is its integration with the broader legal system of norms concerning new technologies, such as the General Data Protection Regulation (GDPR), product liability regulations, cybersecurity, and specific sectoral requirements. As a result, the AI Act establishes a broad legal framework that sets out principles for all systems that could, firstly, be considered as artificial intelligence systems, taking into account their impact on fundamental rights, security, and social trust, as well as defining requirements regarding transparency, accountability, and oversight of their application or, secondly, could be components of other products [Bakiner 2023, 558-82]. Therefore, it should also be read, interpreted, and applied alongside other provisions, such as regulations concerning data protection (e.g., GDPR), product liability, cybersecurity, and sectoral standards, ensuring coherence and compliance with the existing legal order (Regulation 2024/1689, Article 59).

The message of the AI Act is to regulate digital development, which will have a long-term impact on political, security, and legal cultures. The regulation applies to both society and economic entities operating within the European market concept, as well as outside it. Its implementation affects all those functioning in the European economic space. This includes technology providers, developers, tools for building systems, as well as issues related to usage fees that may affect market value. Responsibility for the implementation of the system lies with the person or institution that purchases and introduces it. For example, a bank acquiring an employee evaluation tool, a school using a management system, or even society as a whole – all are subject to the same rules.

In this context, the political culture aspect strongly resonates, as political decision-makers, through the introduction of regulatory standards, aim to ensure the protection of citizens' rights and provide transparency and accountability in the application of AI [Kushe 2024, 1-14]. Equally important is ensuring a balance between innovation and the protection of the public interest. Governments also introduce control mechanisms to minimize the risks associated with the unpredictable development of AI. This is directly linked to the values defining the approach to risk management, which fits within the framework of security culture.

With the establishment of new regulatory frameworks at the European level, new obligations are introduced for AI providers and users, which could become a model for future regulations. It is worth noting that the very implementation will require adjusting the legal systems of EU member states and continuous evaluation to keep pace with the dynamic technological development. This, in turn, expands and develops the space of legal culture.

On the margins of these considerations, it is worth noting that the law may not keep up with the pace of technological development, which advances very quickly. This is a common issue, especially in the context of technological progress, when regulations quickly become outdated. Many legislative actions, like in the case of the European Union, foresee the creation of codes of conduct by associations of companies or industry sectors. This provides greater regulatory flexibility to keep pace with technological advancements, of course, with the appropriate institutional arrangement so that the state can approve these self-regulatory frameworks. This is one method of addressing this issue, but also an additional factor that enriches and develops legal culture.

The discussion of the European AI regulation (Regulation 2024/1689) as well as the technology itself in the cultural triangle, is a contribution to the ongoing public debate on how to harmonize the implementation of artificial intelligence with democratic and liberal values. Moreover, this issue pertains to the process of Europeanization, meaning that this regulation creates a reference point that could serve as inspiration for other political and economic entities.

The European Union operates in the international space according to the principles of integration or Europeanization, meaning that the hegemon sets the rules and knows what it wants to achieve for its interests, which in turn should strengthen Europe's position in promoting global principles. The integration process is carried out in relation to the 27 states, each of which has different positions, opinions, and varying strength and influence in the European Parliament. However, the foundation is that all have committed to adhering to common values such as the rule of law, democracy, and the protection of fundamental rights. In other words, they are building a common political, security, and legal culture based on unified rules regulating the application of new technologies, including artificial intelligence. As a result, it becomes possible to harmonize the approach to innovation, the protection of citizens' rights, and the management of risks associated with digitization.

On the other hand, Europeanization in the context of AI refers to the influence of EU regulations, norms, and values on member states as well as other entities, including countries outside the EU. As is often the case with European regulations, it will have a spreading effect on the rest of the world. This will allow for the assessment and analysis of the impact that this European initiative may have on the international stage. The AI Act has extraterritorial effects, meaning that it applies to organizations outside the EU, provided that the system is used within the EU. This means that systems designed in the United States, China, or elsewhere, if used within the EU, must comply with the regulation [Carver 2024].

The ambition of the authors of this document is for the regulations it contains to have an international character, standardizing the use of AI in accordance with fundamental human rights. The AI Act introduced based on the fundamental rights of the EU is the first global legislation on artificial intelligence and also aims to have an external effect, so that the European concept and European values, as well as respect for universal values, serve as a model for entities outside the EU. Many countries around the world are very interested in artificial intelligence and are also developing their own rules, which the European Union has decided to define, establishing principles that will be applied based on the risks associated with artificial intelligence in various systems.

## 4. RISK MANAGEMENT IN AI: BETWEEN THE CULTURE OF SECURITY AND THE CULTURE OF LAW

The threats and risks of certain harms generate preventive actions, which sometimes use innovative, pioneering solutions. In doing so, they initiate progress both in the development of technological knowledge and in fostering new perceptions, horizons of thought, and the shaping of new social attitudes, which in turn influences the emergence of new norms and regulations. This compulsion to codify and record expected behaviors affects not only the creation of new areas of legal culture but also of security culture. This confirms that culture is a dynamic, living, and evolutionary field, subject to continuous, uninterrupted change.

As is widely known, AI, despite its numerous advantages, also presents significant challenges and risks. Of course, systems deemed to pose unacceptable risk will be excluded from the market. However, in the case of systems considered to be risky but acceptable, a certification process for compliance will be required. This process will include audits conducted by independent, external entities, whose task will be to assess whether a given system meets the required standards. Only after receiving certification will these systems be allowed to enter the market (Regulation 2024/1689, pt. 67).

The AI Act categorizes artificial intelligence systems based on groups depending on the varying levels of risk assigned to systems within each group, according to the risk assessment previously established by the regulatory bodies of the European Union. It distinguishes four main categories: unacceptable risk (prohibited AI systems) (Regulation 2024/1689, Article 5), high risk (systems subject to strict regulation) (Regulation 2024/1689, Article 6), limited risk (systems requiring transparency), and minimal risk (systems not requiring special regulation) (Regulation 2024/1689, pt. 138). Therefore, despite the ban on practices that create acceptable risks to fundamental rights in terms of safety and health, there exists a higher-risk artificial intelligence system that will require specific requirements and obligations from various entities involved in the AI supply chain.

In other words, the first level is unacceptable risk, which has simply been prohibited. This pertains to everything related to social scoring, people's privacy, and other associated areas. The second level of risk is high or very high risk, and systems falling under this category will be subjected to compliance checks and tests before they are actually introduced to the market. Then, there is the third level, which also carries specific obligations for systems that have direct contact with people, requiring transparency and the identification and labeling of products generated by artificial intelligence. Finally, there is the fourth risk category, which is associated with what is called minimal risks, where the risk is relatively small and does not require any special regulations.

## 5. WHERE DOES THE EUROPEAN UNION DRAW THE BOUNDARIES OF AI?

In this section of the paper, we aim to more precisely identify several applications of artificial intelligence that are prohibited at the European level. This area of regulation is crucial from both a legal and security perspective, as it seeks to predict future threats, thereby enriching the framework of meaning of this concept. The introduction of systems such as chatbots, conversational AI, and other similar systems, which are highly popular in the development of artificial intelligence, can lead to serious potential risks associated with this technology.

According to the European Commission's proposal, AI systems posing an unacceptably high risk, which threaten human safety, will be prohibited. This includes systems that result in social exclusion. It will also be forbidden to categorize people based on their social behavior or personality traits (Regulation 2024/1689, pt. 46). European regulation expands the scope of prohibitions to include the coercive and discriminatory use of AI, such as: first, biometric identification systems in public spaces for monitoring leisure time or later identification; second, biometric categorization systems using physical and personal characteristics such as ethnic origin, citizenship, or political beliefs; and third, AI systems used by the police for predicting potential behaviors, profiling, location tracking, or monitoring activities. Additionally, systems for emotion recognition in workplaces and educational settings, as well as the unintended collection of facial images from the internet or recording behaviors to create databases for facial recognition, are also prohibited. Defining artificial intelligence is a critical element of the legislative spectrum, as its definition is essential (Regulation 2024/1689, pt. 44).

AI systems based on historical data analysis could lead to the reproduction of past patterns, rather than introducing innovative and fair solutions. As a result, there are several risks, such as the potential for bias, discrimination, and misinformation, which are real and existing threats. Many models currently being implemented carry with them social prejudices.

A controversial issue is remote biometric identification. This mainly concerns facial recognition and other types of identification used by the police and law enforcement agencies. Regulations have been introduced that prohibit real-time remote biometric identification, but there are broad exceptions for law enforcement, which may use this type of AI system in specific cases, such as during the search for a kidnapped child or a terrorist. So, while it is formally prohibited, there are practical ways to circumvent this rule. Nevertheless, a high global standard has been established in limiting the use of these technologies. The main goal here is to ensure that AI does not assess or evaluate citizens in their access to education or employment.

If individuals are assessed by AI, the human factor must be preserved so that a person's life path is not solely determined by machines.

In practice, these concerns are related to very practical issues, such as the possibility of discrimination by AI systems, lack of transparency regarding how they work, and the potential for privacy violations and improper processing of personal data. These are more practical, concrete concerns arising from the various applications of AI in different fields. Every regulation being discussed today addresses these concerns, rather than fears about superintelligence that could dominate humanity. There are many practical concerns related to AI due to the speed at which it is becoming widespread.

It should be noted that an agreement has been reached that in certain very specific areas, biometric identification may be used. Therefore, when someone goes missing, these systems are used to quickly identify certain movements and locate the missing person, or when there is a threat of a terrorist attack, to identify the perpetrators (Regulation 2024/1689, pt. 33).

The geographical and, above all, cultural context is particularly evident when using AI for social scoring, a common practice in China regarding its citizens, whereas in the EU, such actions are prohibited (with the exception of very specific cases for law enforcement, such as when it is necessary to apprehend a suspect in relation to, for example, identifying a kidnapping victim, human trafficking, or a minor, as well as preventing a terrorist attack). The same applies to crime prediction, meaning the use of AI to forecast whether a person will commit a crime. Similarly, bans are in place regarding the use of AI for emotion recognition in education and the workplace. This means that the application of artificial intelligence and the definition of its scope of operation are closely tied to deeply rooted factors in the areas of political, security, and legal culture.

## 6. DISINFORMATION AND AI

It is important to address the potential threats to freedom and democracy. Advanced disinformation campaigns are already being carried out, and they are sure to increase in the future. It is easy to generate deepfakes of politicians saying things they never said or create false information on a massive scale.

Disinformation affects different countries and societies in various ways. In countries with strong institutions (and therefore a much more deeply rooted political culture), such as the United Kingdom or the United States – although they may seem fragile at the moment – there is greater resilience to disinformation than in many other regions of the world where political, social, and media institutions are not trusted. The flip side of this problem is that the more people realize they cannot trust any information, the more problematic the situation becomes. This has become a particularly significant challenge for human rights activists who document war crimes. They now bear a greater burden of proof – they must prove that a video depicting a war crime is authentic. This is a huge problem because people begin to function in a state of suspension, where they don't want to believe anything, and ultimately, they only believe the information that reinforces their pre-existing beliefs.

An interesting case is the conditional use of AI products with clear labeling as creations made by AI. Jessica Rosenworcel, Chair of the Federal Communications Commission (FCC), proposed a regulation requiring broadcasters to disclose the use of artificial intelligence in political advertisements [Rosenworcel 2024]. The proposal seeks input from consumers regarding methods for disclosing information and definitions of AI-generated content. It mandates the disclosure of information both on-air and in writing in political broadcasts and applies to candidate ads and broadcasts, including cable operators, satellite TV providers, and radio. This situation highlights the importance of regulating the use of artificial intelligence in the public sphere, particularly in the context of transparency and the protection of democratic processes, which in turn shapes the area of political culture. These rules are meant to prevent the development of artificial intelligence that could manipulate people subliminally, so essentially, these guidelines aim to prevent manipulation.

## CONCLUSION

In conclusion, it can be stated that culture encompasses principles related to the political, security, and legal systems. Over time, however, the fundamental elements of culture are reinterpreted by external factors, such as technological progress, which contributes to the evolution of this concept and many of its derivative areas of meaning. The popularity of new technologies significantly impacts the surrounding reality, which is why, from this perspective, one can better understand or explain the ongoing processes in the public sphere.

The analysis carried out in this work confirms that technological progress, particularly the development of artificial intelligence, forces the reinterpretation of existing definitions and the revision of practices within these cultures, leading to their mutual permeation. The study also shows that if AI regulations are appropriately designed, they can strengthen civil rights and provide greater protection against abuses. However, the use of algorithms in public life remains a challenge in the fields of politics, security, ethics, and law, as it involves issues of transparency, discrimination resulting from algorithms, and the risk of violating privacy.

The dynamic pace of technological development presents challenges for legal regulations, while simultaneously affecting democratic institutions and social norms. EU regulations on AI aim to regulate its development in the political, legal, and security contexts, integrating technologies with respect for human rights and democratic values. In order to effectively integrate AI into the public sphere, it is necessary to continue the development and adaptation of legal regulations that will harmonize the implementation of innovation with fundamental human rights and democratic values. A valuable recommendation in this context is the promotion of widespread public education about the impact of AI on daily life and supporting research on mechanisms for controlling and balancing technological development. In the European context, it is important to focus on further integrating the principles of Europeanization, which can serve as a model for other regions when developing their own legislative frameworks.

## REFERENCES

Antoszewski, Andrzej, and Ryszard Herbut (eds.). 1999. *Leksykon politologii*. Wrocław: Alta2.

Bakiner, Ozan. 2023. "Pluralistic Sociotechnical Imaginaries in Artificial Intelligence (AI) Law: The Case of the European Union's AI Act." *Law, Innovation and Technology* 15, no. 2:558-82.

Bankowicz, Marek (ed.). 1999. *Słownik polityki*. 3rd ed. Warszawa: Wiedza Powszechna.

Blackburn, Simon (ed.). 2004. *Oksfordzki Słownik Filozoficzny*. Scientific Editor Jan Woleński. Warszawa: Wydawnictwo Książka i Wiedza.

Carver, John. 2024. "More Bark Than Bite? European Digital Sovereignty Discourse and Changes to the European Union's External Relations Policy." *Journal of European Public Policy* 31, no. 8:2250-286.

Chauvin, Tatiana, Tomasz Stawecki, and Piotr Winczorek. 2016. *Wstęp do prawoznawstwa*. Warszawa: Wydawnictwo C.H. Beck.

Christou, George, Tobias Meyer, and Riccardo Fanni. 2024. "The European Union: Assessing Global Leadership through Actorness in Artificial Intelligence." *Journal of European Integration* 47, no. 3:383-401.

Crawford, Kate. 2021. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven–London: Yale University Press.

Dereń, Ewa, and Edward Polański (eds.). 2008. *Wielki Słownik Języka Polskiego*. Kraków: Krakowskie Wydawnictwo Naukowe.

Hunter, Lauren Y., Christopher D. Albert, Jessica Rutland, et al. 2024. "Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia Are Using Artificial Intelligence in Their Information Warfare and Influence Operations." *Defense & Security Analysis* 40, no. 2:235-69.

Janowski, Jacek. 2012. *Cyberkultura prawa. Współczesne problemy filozofii i informatyki prawa*. Warszawa: Difin.

Kushe, Isabel. 2024. “Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk.” *Journal of Risk Research*, 1-14.

Misiuk, Andrzej, Jolanta Itrich-Drabarek, and Magdalena Dobrowolska-Opała (eds.). 2021. *Encyklopedia bezpieczeństwa wewnętrznego*. Warszawa: Elipsa.

Olechnicki, Krzysztof, and Paweł Załęcki. 1997. *Słownik socjologiczny*. Toruń: Wydawnictwo Graffiti BC.

Pham, Bao C., and Stuart R. Davies. 2024. “What Problems Is the AI Act Solving? Technological Solutionism, Fundamental Rights, and Trustworthiness in European AI Policy.” *Critical Policy Studies*, 1-19.

Polański, Edward (ed.). 2008. *Słownik Języka Polskiego*. Kraków: Krakowskie Wydawnictwo Naukowe.

Purcell, Zachary A., and Jean-François Bonnefon. 2023. “Research on Artificial Intelligence Is Reshaping Our Definition of Morality.” *Psychological Inquiry* 34, no. 2:100-101.

Radanliev, Petr. 2025. “AI Ethics: Integrating Transparency, Fairness, and Privacy in AI Development.” *Applied Artificial Intelligence* 39, no. 1. http://dx.doi.org/10.2139/ssrn.5267574

Rosenworcel, Jessica. 2024. “Proposes AI Disclosure for Political Ads on TV & Radio.” https://www.fcc.gov/document/rosenworcel-proposes-ai-disclosure-political-ads-tv-radio [accessed: 31.03.2025].

Szymczak, Mieczysław (ed.). 1995. *Słownik Języka Polskiego*. Warszawa: PWN.

Szymczak, Mieczysław (ed.). 2000. *Słownik Języka Polskiego*. Warszawa: PWN.

Tokarczyk, Roman. 2000. *Współczesne kultury prawne*. Kraków: Zakamycze.

Walicka, Bogumiła (ed.). 2008. *Słownik politologii*. Warszawa: Wydawnictwo Naukowe PWN.

Żmigrodzki, Piotr (ed.). 2003. *Wielki słownik frazeologiczny*. Warszawa: PWN.

Żmigrodzki, Marek, and Wojciech Sokół (eds.). 1999. *Encyklopedia politologii*. Vol. I: *Teoria Polityki*. Zakamycze: Wydawnictwo Zakamycze.