UNDER THE SIGN OF INTELLIGENCE. HUMAN RIGHTS IN THE ERA OF ARTIFICIAL INTELLIGENCE: REVOLUTION OR ILLUSION?

Aliases: Mihai CÎRPACIU*, Ramona ISTRATE*, and Iosefina CIUREA*

ABSTRACT

What happens to human rights when decisions are no longer made in courtrooms, but behind the algorithm? Does Artificial Intelligence represent a promise of the future or a constant presence, capable of redefining existential paradigms? In this world, rewritten in binary language, freedom, dignity, and privacy are part of a power game that they did not choose. The article examines how algorithms can serve as allies of justice, yet also become actors of programmed exclusion. From cases of algorithmic discrimination to mass surveillance systems, the work questions the compatibility between AI and the fundamental values of humanity. In a landscape dominated by the illusion of transparency and dictated autonomy, technological performance is not the real stake, but rather our ability to keep the citizen at the center of the decision-making process. Artificial Intelligence may be a revolution, but in the absence of well-founded ethics, it risks becoming just another illusion.

Keywords: *artificial intelligence, human rights, digital rights, digital ethics, emerging technologies.*

* Student at the Faculty of Intelligence Studies, "Mihai Viteazul" National Intelligence Academy, Bucharest
* Student at the Faculty of Intelligence Studies, "Mihai Viteazul" National Intelligence Academy, Bucharest
* Student at the Faculty of Intelligence Studies, "Mihai Viteazul" National Intelligence Academy, Bucharest, and at the Faculty of Cybernetics, Statistics, and Economic Informatics, Academy of Economic Studies, Bucharest

Introduction

The contemporary landscape is shaped by an unprecedented acceleration of technology, where Artificial Intelligence (AI) stands not only as an auxiliary tool for progress but as an active agent in a paradigmatic shift. In its operational sense, AI refers to a broad spectrum of systems capable of replicating human cognitive processes-such as learning, reasoning, and adaptation-through algorithmic programming, generative neural networks, or advanced data processing models (Goodfellow, Bengio, & Courville, 2016). From image analysis with OpenCV to predictive modeling using TensorFlow or audio interpretation via Librosa, AI is now infiltrating the most delicate layers of social and personal reality.

Yet, along with these technological advances, a host of challenges also arise. As AI gains increasing autonomy in decision-making, we begin to see potential collisions between algorithmic logic and the foundational values of human rights. These rights, rooted in the struggles for freedom, dignity, and justice, remain the structural pillars of international law and universal ethics. In an era where algorithms assess legal claims, approve or deny credit, monitor behavior, and influence political opinion, protecting these rights is not simply prudent; it is essential.

This article examines how AI might respect, threaten, reinforce, or reshape core human rights. It highlights two key responsibilities: first, to understand how emerging technologies align or conflict with the values that formed modern civilization; second, to acknowledge the duty we have in developing and managing AI systems in ways that protect human dignity. As artificial intelligence takes on an increasingly important role in shaping social, economic, and political outcomes, we must ask: can these systems truly uphold fundamental human rights? Or is it solely our responsibility to guide, constrain, and educate AI in an ethical manner? AI, by its very nature, has no innate understanding of morality or legitimacy. It is not self-aware, nor inherently ethical. It simply reflects the values, assumptions, and goals of those who create and use it. In this way, algorithmic systems serve both as a mirror of our intentions and potential agents of profound social change, some of which could disrupt the balance of human communities.

This paper aims to explore the delicate balance between the emancipatory potential of artificial intelligence and the risk that it may reduce humans to mere objects of digital processing. It is, at its core, a deliberate effort to reaffirm the importance of human rights in shaping the structure of our new digital order.

AI and human rights

To comprehend how we might transform AI from a disruptive force in citizen–state relations into a catalyst for societal progress, we must confront a pressing question: What should we do when AI morphs from an ally to an adversary? If we paused for a moment from our daily routines, we would realize that artificial intelligence no longer resides solely in science fiction or distant-future narratives. It is embedded in medical decisions, in the curation of our news feeds, and in algorithms that determine what we see and hear. We no longer ask whether AI will impact our lives; instead, we ponder how it does so and, more critically, what space remains for our rights and freedoms when the rules of engagement are increasingly dictated by code. Initial interactions with these technologies were marked by optimism. In medicine, research led by Esteva et al. (2017) demonstrated that machine learning algorithms could detect melanoma with accuracy comparable to that of dermatologists, offering real prospects for early diagnosis, especially in regions lacking medical infrastructure.

In education, adaptive systems, as described by Luckin et al. (2016), introduce the concept of personalized learning paths tailored to each student's pace and needs. For the first time, children were no longer limited to uniform learning environments; algorithms became invisible mentors, capable of adjusting educational trajectories in near real-time. In the area of human rights, organizations such as Amnesty International (2019) have utilized automated satellite image analysis to document human rights violations in inaccessible areas. In such cases, AI served as both witness and protector, stepping in where human observers could not. However, this promising image has a darker side. Studies by Buolamwini and Gebru (2018) showed that commercial facial recognition systems had disproportionately higher error rates for women and people of color. Discrimination no longer shows up in obvious ways but subtly infiltrates data models and algorithmic results, continuing old injustices and changing how racial disparities are expressed.

A more significant challenge is the opacity of these systems. Pasquale (2015) warns of the "black box" phenomenon, where algorithms make life-altering decisions without their internal logic being understandable or contestable. How can a justice system function when the basis of decisions remains hidden from those affected? Recent examples highlight this systemic issue. Clearview AI, a company that collected millions of biometric images without explicit consent, sparked significant legal and ethical debates regarding the right to privacy. In the U.S. judicial system, the COMPAS algorithm, designed to predict recidivism, faced criticism for reinforcing racial biases, undermining the principle of equality before the law.

In another context, analysis of China's social credit system by Creemers (2018) illustrates how algorithmic technologies can become subtle yet relentless tools of social control. Evaluating individual behavior based on automated parameters not only redefines the concept of citizenship but also risks eroding personal autonomy. China's use of AI extends beyond individual behavior assessment; it employs these tools disruptively, directly impacting personal freedoms. During the COVID-19 pandemic, Chinese authorities implemented large-scale automated citizen classification systems based on presumed epidemiological risk. Through mobile phone-integrated monitoring apps, individuals were assigned color codes (green, yellow, or red) that determined, in real-time, their ability to move freely, need for quarantine, or complete restriction from public spaces. This classification, often irrefutable, turned algorithms into arbiters of freedom of movement. Moreover, non-compliance with rules imposed by these systems was automatically sanctioned: surveillance cameras and connected data networks identified individuals not wearing masks or failing to maintain social distancing, issuing fines without human intervention. Thus, public spaces became arenas of constant monitoring, where technology evolved from a public health aid to an instrument of continuous control and punishment.

Given this reality, it becomes clear that technology is not impartial. Artificial intelligence mirrors the values, priorities, and inequalities of the society that develops it. Recognizing this requires a re-evaluation of the relationship between technology and human rights within a normative framework that tackles the challenges of the digital age. Digital rights in this transformed cyberspace include the right to protect personal data, transparency in algorithms, and informational diversity. These are no longer just extensions of traditional rights; they are the foundation of freedoms in the digital world. The right to privacy goes beyond protecting one's home or correspondence—it involves control over data generated continuously by online activity. Freedom of expression means not only the right to speak but also protection from algorithmic marginalization in an information space governed by unseen algorithms. In the age of networks and platforms, true freedom depends on access to a safe and fair digital environment.

This transformation requires a redefinition of the social contract. Traditionally, the state was the protector of fundamental rights. Today, technological platforms, data corporations, and algorithmic systems have become *de facto* normative influencers. Any renewal of the social contract must acknowledge this reality: establishing clear ethical boundaries, ensuring transparency in decision-making, and empowering individuals to have real control over their data. The European Union, through initiatives such as the General Data Protection Regulation (GDPR) and recent proposals for AI regulation, has begun to shape the contours of this new agreement. UNESCO (2021) has also proposed a global ethical framework for the responsible development and use of artificial intelligence, promoting explainability, fairness, and respect for cultural diversity. However, these efforts are just the beginning. Their success depends not only on defining principles but also on their practical application amid economic interests and geopolitical considerations. It is valid to ask: How can we build algorithmic systems that correct injustices instead of continuing them? How do we make sure that new forms of digital power stay compatible with human dignity and personal freedom? The answers are complicated and can't come only from the IT sector or lawmakers. They need widespread involvement from civil society, increased citizen awareness, and a public culture that critically examines technology. In this way, artificial intelligence can truly become an extension of humanism rather than a subtle form of dehumanization.

Private in name only. Artificial Intelligence and the decline of privacy: GDPR vs. AI

The General Data Protection Regulation (GDPR) governs how EU citizens' personal data is collected, stored, processed, and protected, aiming to safeguard their rights and privacy. This regulation influences the development and deployment of artificial intelligence (AI). Although GDPR seeks to protect consumer data, it may limit AI innovation in Europe, potentially putting EU companies at a competitive disadvantage (Wallace & Castro, 2018). Many organizations struggle to fully comply with the

GDPR, particularly when adopting AI technologies, due to the regulation's complexity and novelty (Addis & Kutar, 2020). GDPR presents challenges for implementing automated decision-making and profiling, creating a responsibility for organizations to balance fostering technological innovation with protecting personal data. As a result, the rules require strict transparency, accountability, and control mechanisms to prevent risks like discrimination, automated errors, and unauthorized data use, all while respecting individuals' fundamental rights in a rapidly changing digital landscape and an era of speed (Mougdir, 2020). However, AI technologies can also assist in ensuring GDPR compliance through rule-based systems and machine learning techniques. These AI tools can aid in compliance checklists, risk assessments, automated profiling regulations, and breach detection and reporting (Kingston, 2017). As AI continues to develop, finding a balance between innovation and data protection remains a key challenge for organizations seeking to remain compliant with the GDPR.

In the professional environment, risks are associated with the use of conversational interfaces based on artificial intelligence, including the potential to violate the General Data Protection Regulation (GDPR). Using virtual assistants, such as ChatGPT (OpenAI), Cursor, Cody, Claude (Anthropic), or Copilot (Microsoft), can be helpful in the context of large files to save time. However, this practice also involves risks and vulnerabilities related to data privacy. To prevent incidents related to the uncontrolled use of AI chatbots, organizations must adopt strict and well-founded measures. A first step is to establish clear policies on the use of these technologies by employees, ensuring a coherent and responsible operational framework. It should also be explicitly stated which types of data can be processed through these systems to reduce risks related to personal data protection. Additionally, organizations must actively work with chatbot providers to ensure that data entered into the system is not stored or used improperly, thereby safeguarding the confidentiality of the information. In the event of a data security incident resulting from unauthorized use of an AI chatbot, organizations have clear legal responsibilities to thoroughly document the incident and immediately notify the relevant authority, either the National Authority for the Supervision of Personal Data Processing (ANSPDCP) in Romania or the European Data Protection Board (EDPB) in the European Union. In some instances, companies must also inform the affected individuals, ensuring transparency and respecting their rights in accordance with GDPR regulations.

The digital footprint, the invisible trace of an increasingly exposed life

With every moment spent online, whether reading the news, shopping for clothes, or scrolling aimlessly through social media, we leave behind a trail of data. These are not just conscious inputs we choose to share, but fragments of ourselves: geolocation pings, click patterns, access frequencies, social interactions, navigation behavior (Bassi, 2020). Once aggregated, they form what is now known as a *digital footprint*.

What is essential to understand is that this footprint is not just metadata. It becomes an invisible double of the real person, one that can be stored, analyzed, and used independently of any informed consent. Even more unsettling is that this shadow rarely remains inert. It is mined, processed, and fed into predictive systems that, silently but decisively, influence our access to services, opportunities, and even visibility in the digital public sphere (Zuboff, 2019). As Shoshana Zuboff poignantly notes in her analysis of surveillance capitalism, "human experience has been claimed as free raw material for translation into behavioral data" (Zuboff, 2019, p. 8). This shift poses not only commercial risks, but it also rewires the foundations of power. Without any real control over how our data is collected or interpreted, we become increasingly vulnerable to manipulation, classification, and algorithmic exclusion—often without knowing, and even more often, without a meaningful way to resist.

We are not just dealing with a privacy issue. We are facing a fundamental threat to the concept of personal autonomy. When decisions are made based on algorithmically generated profiles, whether related to credit access, employment prospects, or the spread of our opinions in digital spaces, the scope of freedom shrinks. And it does so quietly, without user awareness, transparency, or meaningful options for response. Even more concerning, these profiles can reproduce or magnify systemic bias. Algorithms trained on incomplete or biased data often end up excluding individuals or groups from opportunities, not out of malice but due to hidden design flaws in the code.

In this landscape, the right to privacy cannot be seen just as protection of one's home or communications. It must be redefined as the right to control how one's digital identity is portrayed, analyzed, and exploited. The lack of clear legal tools to defend this representation not only exposes intimacy but also erodes dignity.

Concepts like the *right to be forgotten*, algorithmic transparency, and personal data ownership are not theoretical luxuries. They are essential mechanisms in the fight to preserve human agency in the age of predictive analytics. Protecting one's digital footprint is not about clinging to nostalgia. It is about making sure no person is reduced to a series of probabilistic assumptions. And in this fight, we are not just defending privacy; we are defending the right to remain unknowable machines.

The path between fairness and credibility

Despite the recognized societal importance of ethics in the field of artificial intelligence, research on public attitudes toward this issue remains limited. This gap is evident in situations where the ethical development of AI is expected to prioritize the collective good of society. For example, some studies show that, while Germans generally see ethical principles as equally important, they find it difficult—if not impossible—to implement them all at once. These groups differ significantly not only in which attributes they prefer but also in how important they consider each attribute (AI-Ethics by Design. Evaluating Public Perception on the Importance of Ethical Design Principles of AI, Kimion Kieslich, Birte Keller, Christopher Starke). Scandals, such as Snowden's revelations about mass surveillance by US intelligence agencies (Steiger et al., 2017) or Cambridge Analytica's collection of data from millions of Facebook users for targeted advertising and election interference in the 2016 US presidential election (Hinds et al., 2020), have recently sparked public outrage. As a result, public focus has shifted toward privacy concerns, and policymakers have increasingly taken steps to address these issues. Shortly after the Cambridge Analytica scandal became public, the European Union implemented the General Data Protection Regulation, marking a significant step toward global policy convergence and fostering a shared understanding of how to handle personal data worldwide (Bennett, 2018).

As artificial intelligence (AI) becomes increasingly integrated into society, emerging ethical concerns related to values such as respect for fundamental rights also arise, along with the social responsibility of technology developers and users. Some of these issues are especially urgent when they involve automated decisions, algorithmic bias, data protection, process transparency, and safeguarding individual autonomy. Automated conclusions based on discriminatory information can reinforce existing prejudices and biases against fairness. Likewise, the extensive collection of personal data raises potential privacy and informed choice issues that must be addressed through precise regulation and strong protections.

At the same time, transparency in how algorithms work makes it more challenging to assign responsibility, especially when AI decisions have a significant impact on people's lives. Therefore, creating explainable and auditable systems where human accountability is central is essential. Additionally, the predictive use of AI can impact individual autonomy by altering access to opportunities and options, thereby risking the reinforcement of existing social inequalities. Furthermore, the extended use of AI can introduce cognitive biases. However, AI also provides significant benefits such as improved efficiency, personalized services, and progress in areas like medicine and mobility. To ensure these advantages are not overshadowed by disruptive impacts, it is crucial that AI development is guided by strong ethical principles, transparency, and effective oversight regulations.

Artificial intelligence must be developed and utilized in a manner that respects human dignity and promotes social justice. Only through an interdisciplinary approach, where values shape technology, can AI help create a fair and inclusive society (Bidașcă, 2023).

Digital rights – the extension of fundamental rights

In the context of growing digitalization and the expansion of artificial intelligence-based technologies, establishing and strengthening the concept of digital rights is essential for protecting individual fundamental freedoms. While new technologies promote innovation and progress, they also create new threats to confidentiality, personal autonomy, and fair access to information, challenging traditional legal and human rights frameworks. Digital rights are not a completely separate set of rights but are instead a translation and extension of rights outlined in documents like the Universal Declaration of Human Rights or the European Convention on Human Rights, adapted to the digital age. Therefore, rights such as privacy, freedom of expression, data protection, and non-discrimination need to be reinterpreted in light of new forms of algorithmic interaction and cyber surveillance.

The concept of digital rights has become an important topic in the digital and information technology era. Digital rights management (DRM) systems have been developed to protect intellectual property in the digital world, raising questions about balancing private control with easier access to information (Caso, 2006). Digital inclusion is now regarded as a new human right, emphasizing the essential role of access to information and communication technologies in today's society (López & Samek, 2009). The digital age has influenced copyright laws, as technological advances have changed how information is created, shared, and used (Santos, 2008). This shift has led to digital rights being recognized as a new category of civil rights, underscoring the need for legal frameworks to address the unique challenges of the digital environment (Konobeevskaya, 2019). These developments highlight the connection between technology, law, and society in the digital age. Although the European Convention on Human Rights (ECHR) does not explicitly mention "digital rights," several key articles are relevant in the context of new technologies. Article 8 guarantees the right to privacy and has been interpreted by the European Court of Human Rights to protect personal data and online communications, as seen in Podchasov v. Russia (2024), which rejected the demand for providers to create "backdoors" to encrypted data. Article 10, on freedom of expression, is crucial for regulating digital platforms, while Article 13 secures the right to an effective remedy for online violations. Article 14 also prohibits discrimination, including cases involving potentially biased algorithms. Overall, the ECHR provides a flexible framework that safeguards fundamental rights in the digital age, adapting traditional principles to new technological challenges.

The United Nations' approach to digital rights is indirectly governed by various international instruments, such as the Universal Declaration of Human Rights (UDHR), which safeguards the right to privacy and freedom of expression, also relevant in the digital realm. The International Covenant on Civil and Political Rights (ICCPR) ensures the protection of personal data. Additionally, UN resolutions highlight the importance of safeguarding fundamental rights online, especially with the advancement of new technologies. Moreover, the UN Principles on Human Rights and Emerging Technologies suggest that technologies should be used in a way that upholds individuals' fundamental rights.

The European Union plans to adopt a Charter of Digital Rights, outlined in the "European Declaration on Digital Rights and Principles for the Digital Decade," which, although not yet legally binding, provides clear guidelines on ensuring fair and universal access to digital infrastructure, protecting personal data, promoting digital skills among citizens, and maintaining a safe, inclusive, and non-discriminatory online environment.

In the context of the profound transformations brought about by the rapid digitalization of global society, international organizations, national governments, and civil society groups are increasingly working to define a conceptual and normative framework aimed at coherently and fairly regulating the complexities of new technological realities from a human rights perspective. This effort has led to essential proposals advocating for the recognition and protection of digital rights as a natural extension of the fundamental rights established in traditional international legal instruments. Modern researchers emphasize the growing significance of digital rights in international law. Kartashkin (2023) introduces the concept of "digital-information rights," supporting a comprehensive International Digital Code of Human Rights as part of the UN Global Digital Pact. Tillaboev (2024) recommends updating international standards for protecting intellectual property in the digital age, including amending existing conventions and creating new security measures. Brown & Korff (2012) underline the responsibilities of both governments and private companies in safeguarding digital freedoms, suggesting practical steps to protect online free expression and privacy. Overall, these studies highlight the need for updated international legal frameworks to address the challenges and opportunities of the digital age, striking a balance between the protection of human rights and legitimate law enforcement needs.

Digital rights can no longer be seen simply as technical extensions of traditional rights; instead, they must be recognized as essential aspects of modern life in an increasingly technology-dependent society. In a world shaped by rapid digitalization, widespread surveillance practices, automated decision-making, and the rise of digital monopolies, protecting fundamental freedoms in the virtual world is a vital democratic, legal, and ethical responsibility. The digital future should prioritize human values over commercial interests or excessive control.

Conclusions

In a digital landscape dominated by automated decisions and algorithmic surveillance, protecting fundamental rights can no longer be approached with traditional methods. Instead, it requires a profound reconceptualization tailored to new technological realities. While artificial intelligence offers significant opportunities for social progress, it also poses major risks to privacy, autonomy, and equality-risks that arise without solid mechanisms for regulation, transparency, and ethical responsibility. Therefore, digital rights must be recognized as pillars of freedom in the information age, and technological development must be accompanied by ongoing critical reflection focused on human dignity to prevent individuals from being transformed into mere objects of automatic processing. Today, aided by technological advances, we see a world where code creates unseen rules, and algorithms emerge from our dreams and fears. It is a world where the biggest challenge is not just controlling artificial intelligence but making sure humanity stays at the core of technology. The AI era is one where decisions are no longer made in courtrooms but through algorithms and mathematical formulas. The most vital resistance is in constantly reminding ourselves that the goal is not just performance but humanity and dignity. In this way, we can see digital transformation as an extension of humanism rather than an illusion of progress.

REFERENCES:

Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., ... & Zheng, X. (2016). TensorFlow: A system for large-scale machine learning. 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16), 265–283.

Amnesty International. (2019). Decoding surveillance: Human rights impact assessments for AI. Amnesty Tech Report.

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias. ProPublica. Retrieved March 10, 2025, from https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Bassi, A. (2020). Understanding digital footprints: The invisible trail we leave behind. Global Journal of Computer Science and Technology, 20(1).

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1–15.

Caso, R. (2006). Digital rights management e libertà d'informazione. Il diritto d'autore, 70(2), 210–230.

Creemers, R. (2018). China's social credit system: An evolving practice of control. SSRN Electronic Journal. Retrieved March 10, 2025, from https://doi.org/10.2139/ssrn.3175792

Decalex. (n.d.). Decalex – Legal services for data protection and compliance Retrieved March 10, 2025, from https://decalex.ro/

Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115–118. Retrieved March 10, 2025, from https://doi.org/10.1038/nature21056

European Commission. (2021). Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act). Retrieved March 10, 2025, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC020

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

Hill, K. (2020, January 18). The secretive company that might end privacy as we know it. The New York Times. Retrieved March 10, 2025, from https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Kingston, J. (2017). Artificial Intelligence and Legal Liability. Research Handbook on Digital Transformations, 1, 1–16.

Luckin, R., Holmes, W., Griffiths, M., & Forcier, L. B. (2016). Intelligence unleashed: An argument for AI in education. Pearson Education.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1–21. Retrieved March 12, 2025, from https://doi.org/10.1177/2053951716679679

Mozur, P., Zhong, R., & Krolik, A. (2020, March 1). In coronavirus fight, China gives citizens a color code, with red flags. The New York Times. Retrieved March 15, 2025, from https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.

United Nations. (1966). International Covenant on Civil and Political Rights. Retrieved March 17, 2025, from https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. Retrieved March 10, 2025, from https://unesdoc.unesco.org/ark:/48223/pf0000380455

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.