RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
March 12-13, 2026
DOI:10.5281/zenodo.19535674

Respect for Human Rights in European Legislation on the Use of Artificial Intelligence

Bogdan Buneci

Associate Professor, PhD, Law School, Ecological University of Bucharest, Romania
bogdanbuneci@yahoo.ro

Abstract: European regulation of artificial intelligence (AI) seeks to reconcile two objectives that sometimes pull in different directions: on the one hand, the desire to encourage innovation, and on the other, the need to strongly protect fundamental rights (human rights as defined in the European context). At the core of this framework is Regulation (EU) 2024/1689 ("AI Act"), which organizes obligations based on risk: it prohibits certain practices deemed unacceptable, imposes pre- and post-deployment requirements for high-risk systems, and requires transparency for uses where the risk is lower. The AI Act is grounded in the values and rights of the EU Charter of Fundamental Rights and operates alongside existing rules, particularly the GDPR (which it does not replace), including for automated decision-making and impact assessments. The analysis highlights two new elements relevant to rights: (1) the Fundamental Rights Impact Assessment (FRIA), required in certain cases prior to use, particularly in the public sector or in services of public interest; (2) a right to an explanation when an individual decision is based primarily on the output of a high-risk AI system. At the international level, the criteria developed by the European Court of Human Rights—legality, necessity, proportionality, and safeguards against abuse—particularly regarding biometrics and surveillance, serve as a useful benchmark for interpreting and applying the AI Act.

Keywords: Artificial Intelligence (AI), fundamental rights, impact assessment, regulations, European Union

Introduction

The development and use of AI in fields such as the justice system, the labor market, healthcare, education, advertising, migration, and law enforcement can pose real risks to rights: intrusions into private life, discrimination (sometimes unintentional), decisions that are hard to understand, errors that are difficult to challenge, and a power imbalance between those who control the systems and the people affected. In European law, these risks are viewed through the lens of "fundamental rights" and the obligation of public authorities to act in accordance with the EU Charter of Fundamental Rights and the standards of the European Convention on Human Rights (ECHR), in line with the rule of law.

In this context, the European Union adopted the AI Act as a tool for harmonizing the internal market, but with an explicit justification: a high level of protection for fundamental rights and public interests. The regulation was adopted in June 2024 and entered into force on August 1st, 2024, with its implementation phased in until 2027. As of March 2026, certain obligations (e.g., prohibitions on specific practices and AI literacy requirements) are already applicable, while other requirements, particularly for high-risk systems, are set to be fully implemented as of August 2nd, 2026, with transition periods for certain categories.

The objective of this paper is to analyze, from a critical doctrinal perspective, how the AI Act and related regulations (GDPR, the EU Charter, DSA/DMA, and data governance acts) incorporate human rights requirements and how compatible this framework is with relevant international obligations (ECHR and UN guidelines).

The term *"human rights"* is used here in its practical European sense: (i) fundamental rights as primary EU law (the Charter) and as general principles of EU law, and (ii) ECHR standards, as interpreted by the European Court of Human Rights. In practice, the AI Act operates at the intersection of the internal market, fundamental rights, and an administrative approach to technological risk governance.

EU regulations on respect for human rights

Scope and Definitions. The AI Act starts with a "functional" definition of an AI system: a machine-based system with a variable degree of autonomy that can "deduce" how to produce outputs (e.g., predictions, content, recommendations, or decisions) that affect the physical or digital environment. This definition, aligned with international convergence (including the influence of the Organization for Economic Cooperation and Development (OECD) debates during the legislative phase), has direct implications for rights: it delineates which technical objects fall under the regime of obligations and, implicitly, which practices may be subject to prohibitions or compliance requirements.

Regarding the scope of application, the AI Act follows the logic of the internal market (the same rules to avoid fragmentation), but also takes into account the effects within the Union: obligations may also become relevant for actors outside the EU if the outputs of the systems are intended for use in the EU. This approach is consistent with the aim of protecting individuals within the Union. At the same time, the regulation provides for sensitive exclusions (e.g., military, defense, or national security activities) and exclusions that support innovation (e.g., research and development prior to market introduction or commissioning). These exclusions may create "gray areas" where the protection of rights depends more on other instruments (the General Data Protection Regulation - GDPR, the European Convention on Human Rights - ECHR, national law).

The risk-based approach as a protective tool. The AI Act establishes a tiered system: (i) prohibited practices (unacceptable risk), (ii) high-risk systems - subject to pre- and post-use obligations, (iii) transparency obligations for certain systems (limited risk), (iv) all other uses - no additional special requirements (minimal risk), but they remain subject to general rules (GDPR, non-discrimination, consumer protection, etc.). The core principle is proportionality: not all AI uses pose the same risks, so the obligations need not be identical either.

In the category of prohibited practices, the AI Act includes, among others, subliminal or deceptive manipulation that can significantly alter behavior (affecting autonomy and dignity); the exploitation of vulnerabilities (particularly of vulnerable individuals); "social scoring" with unjustified negative effects (risk of discrimination); the assessment of the risk of committing crimes solely based on profiling or personal traits (affecting the presumption of innocence in the broad sense); and expanding facial recognition databases through massive, untargeted collection ("scraping"). Remote, "real-time" biometric identification in public spaces for law enforcement purposes is treated as prohibited, but with limited exceptions and strict procedural conditions (including necessity, authorization, impact assessment).

Classification of high-risk systems and the link to rights. "High-risk" systems are defined both by the fact that they are integrated into already regulated products (for example, as a "safety component," according to the AI Act annexes) and by the listing of certain sensitive areas (for example, education, employment, essential services, law enforcement, migration). The rationale is explicit: assessing the impact on health, safety, and fundamental rights. In this area, protection is achieved through "technical and procedural" requirements: risk management, data governance, documentation, traceability, transparency, human oversight, and robustness.

An important element for rights is the direct link that the AI Act establishes between data governance and the prevention of discrimination. The datasets used for training, validation, and testing must be managed in such a way that biases capable of producing unfair effects on individuals or groups are identified and mitigated. The regulation requires measures to detect, prevent, and mitigate these issues. In this way, part of the obligation of non-discrimination (Charter of Fundamental Rights of the EU, Art. 21) and the principles of "fairness" in the GDPR (Art. 5) are incorporated as early as the design and use stages.

The Fundamental Rights Impact Assessment and its connection to the GDPR (General Data Protection Regulation), DPIA (Data Protection Impact Assessment). A key innovation

for ensuring compliance with fundamental rights is the Fundamental Rights Impact Assessment (FRIA), which is required prior to the use of certain high-risk AI systems. The obligation primarily applies to: (i) implementers that are public authorities/bodies or private entities providing public services, and (ii) certain systems used in areas where decisions may directly affect the existence of and access to services (e.g., certain uses in the *"essential services*" sector). The AI Act requires: a description of the system's use (purpose, duration, frequency), who may be affected (categories, groups), what specific risks arise for rights, and what measures are in place (human oversight, internal procedures, including complaint mechanisms).

The correlation with the GDPR is explicit: the AI Act states that when a Data Protection Impact Assessment (DPIA), conducted in accordance with Article 35 of the GDPR, already covers certain requirements, the FRIA should not duplicate that analysis but rather supplement it. In practice, a model of "integrated due diligence" is emerging: (a) the DPIA focuses on risks related to personal data, (b) the FRIA takes a broader view of other rights (non-discrimination, access to services, procedural rights, the right to defense). In practice, this division helps avoid a discussion that remains confined to "privacy" alone, ignoring other rights.

Transparency and information: from the "right to know" to labeling synthetic content. The AI Act has two layers of transparency. The first concerns high-risk systems: they must be designed so that users can understand and correctly interpret the results, and user instructions must clearly state the purpose, limitations, accuracy, robustness, and foreseeable misuse scenarios. The second layer, more visible to the public, concerns use that interact directly with people: the obligation to inform that the interaction is taking place with an AI system, rules for generative systems (labeling content as artificially generated or manipulated), and obligations for deepfakes (disclosure of synthetic nature), with exceptions for law enforcement and adjustments for artistic or satirical content.

From a rights perspective, these obligations aim to reduce:

(i) lack of transparency and information asymmetry (autonomy, informed consent);

(ii) risks of manipulation and disinformation (freedom of opinion formation, integrity of the democratic process);

(iii) damage to reputation and privacy related to synthetic content.

However, where exceptions exist (particularly for law enforcement), they must be interpreted strictly and accompanied by effective safeguards. If transparency is limited, control through authorization with clear limits and independent oversight becomes all the more important.

Human oversight and accountability. The AI Act treats human oversight as a mechanism for mitigating risks to health, safety, and rights. It is not just about "who presses a button," but also about how human-machine interfaces are designed and what organizational measures are in place. Specifically, implementers' obligations include: using the system according to instructions, designating competent individuals for supervision, monitoring operations, maintaining logs, reporting incidents, and informing workers (and their representatives) before using high-risk systems in the workplace. This obligation links technological governance to social and procedural rights (information, participation, privacy at work).

Remedies and "procedural rights" in the AI Act. Unlike the GDPR, which provides a comprehensive set of data subject rights and remedies, the AI Act introduces a more limited but significant core of remedies. Two provisions are central to the human rights perspective: (1) the right to file a complaint with the market surveillance authority, for any person (natural or legal) who has reason to believe that the Regulation has been violated; (2) the right of a data subject to request "clear and meaningful" explanations regarding the role a high-risk AI system played in making a decision and the main elements of that decision, when the decision

produces legal effects or significantly affects the individual (e.g., in relation to health, safety, or fundamental rights). This right applies only to the extent that EU law does not already provide an equivalent right, suggesting an intention to avoid overlap with the automated decision-making regime under the GDPR.

From the perspective of the EU Charter of Fundamental Rights (Art. 47 - the right to an effective remedy), these mechanisms are useful, but they also raise questions about their practical effectiveness. An explanation of the system's "role" and the elements of the decision does not, on its own, guarantee access to sufficient details to effectively challenge the outcome (e.g., access to relevant data, the reasoning used, or audits), especially when claims of trade secrets are invoked or when the systems are used in law enforcement.

Correlations between the AI Act and related regulations: GDPR, the Charter, DSA, DMA, the Data Governance Act, and the Data Act

With regard to the GDPR, the AI Act expressly states that it is complementary and does not, in and of itself, create a new legal basis for the processing of personal data. This is essential for AI systems trained on personal data: the principles of the GDPR (lawfulness, fairness, transparency, data minimization, accuracy, and storage limitation), the rules regarding special categories (e.g., biometric data), and the regime governing automated decision-making and profiling remain applicable.

In relation to the Charter of Fundamental Rights of the European Union, the AI Act functions as a sector-specific instrument that puts certain rights into practice in a technological context. The following are particularly relevant: privacy and data protection (Art. 7-8), non-discrimination (Art. 21), the rights of the child (Art. 24), and the right to an effective remedy (Art. 47). The rule on the limitation of rights (Art. 52) is particularly important when the AI Act provides for exceptions, for example in the field of law enforcement.

With regard to the *Digital Services Act (DSA),* there are functional overlaps in the areas of procedural rights and algorithmic transparency in the online environment. The DSA imposes obligations regarding content moderation, complaint-handling mechanisms, and explicit references to the right to an effective remedy (Charter, Art. 47), as well as to international standards such as the UN Guiding Principles on Business and Human Rights (UNGP). For platforms that use AI for recommendations or moderation, the DSA can complement the AI Act with procedural safeguards and obligations to assess and mitigate societal risks.

In relation to the *Digital Markets Act (DMA),* the restrictions on the combination and cross-use of personal data (particularly in online advertising), which are contingent on consent and the availability of a less personalized alternative, are of particular importance. These rules directly influence the profiling ecosystems that power many AI applications (scoring, targeting). In this regard, the DMA can indirectly support privacy rights and data protection by reducing the structural pressure toward excessive data accumulation.

In relation to the Data Governance Act (DGA) and the Data Act, both instruments reaffirm that European Union law on the protection of personal data takes precedence when a conflict arises and that these acts, as a rule, do not create autonomous legal grounds for the processing of personal data. For AI, these regulations can facilitate access to data, including through data-sharing frameworks, but at the same time, they introduce limits and conditions that can support the protection of rights: data minimization, protection of sensitive data, governance rules, and control mechanisms.

Interaction with ECHR case law and international standards

In the context of international obligations, the ECHR and the Court's case law establish useful criteria for assessing whether the use of AI is compatible with human rights: the existence of an

accessible and predictable legal basis (legality), necessity in a democratic society, proportionality, and effective safeguards against arbitrariness, accompanied by effective independent oversight. These criteria are essential for interpreting the AI Act, especially in areas where exceptions or intrusive uses arise (such as biometrics, surveillance, and law enforcement).

A landmark case is *S. and Marper v. the United Kingdom* (European Court of Human Rights, 2008). The Court examined the indefinite retention of fingerprints and DNA profiles of unconvicted individuals, emphasizing the sensitivity of biometric data and the risk of stigmatization, as well as the danger of a disproportionate intrusion into private life. For AI ecosystems, the significance is twofold: (i) the construction and maintenance of biometric databases and (ii) their subsequent use in automated identification. The AI Act, through its ban on mass, untargeted data collection ("scraping") for facial recognition databases and its restrictions on real-time remote biometric identification, can be understood as an attempt to prevent such abuses.

In *Big Brother Watch and Others v. the United Kingdom* (European Court of Human Rights, 2021), the Court examined mass interception and information-sharing regimes, emphasizing "end-to-end" safeguards (from authorization through to selection, storage, access, and oversight). From an AI perspective, the case shows that a general legal basis is not sufficient: institutional and procedural mechanisms are needed to limit arbitrariness and enable verification (auditability). This lesson is relevant to the AI Act in two ways: (i) how exceptions in the application of the law are justified and controlled, and (ii) why the governance and oversight architecture at the EU level (e.g., the AI Board and the AI Office) matters for systemic risks.

The case of *Glukhin v. Russia* (European Court of Human Rights, 2023) is directly relevant to biometrics and protest. The Court examined the use of facial recognition to identify and arrest a protester, highlighting how intrusive the technology can be and the risk of a "chilling effect" on freedoms. For the AI Act, this case law supports a strict interpretation of the conditions of necessity, temporal and spatial limitation, authorization, and oversight, as well as heightened attention to the effects on the freedoms of assembly and expression.

In addition to the ECHR, the Council of Europe (2024) adopted the *Framework Convention on AI*, Human Rights, Democracy, and the Rule of Law, which was opened for signature on September 5, 2024. It is the first legally binding international treaty dedicated to AI. The Convention reinforces principles such as dignity and autonomy, transparency and oversight, accountability, equality, and non-discrimination, and calls for graduated measures based on severity and probability. Overall, it aligns with the AI Act (risk-based approach, transparency requirements, accountability), but may also raise the bar where the AI Act remains more sector-specific and more reliant on market oversight.

At the UN level, the relevant guidelines do not generally function as directly applicable law within the European Union, but they do provide standards of due diligence and interpretive benchmarks. The *UN Guiding Principles on Business and Human Rights* (United Nations, 2011) articulate the "Protect-Respect-Remedy" triad, requiring states and businesses to prevent and remedy adverse impacts on rights, including through impact assessments and grievance mechanisms. The DSA explicitly refers to these principles in the context of platform due diligence; the AI Act, through FRIA and the right to complaint and explanation, moves in a similar direction but lacks the same level of detail for the entire lifecycle of AI systems.

The United Nations Educational, Scientific and Cultural Organization (UNESCO, 2021), in its *Recommendation on the Ethics of Artificial Intelligence*, and materials from the Office of the UN High Commissioner for Human Rights (OHCHR, 2024) on privacy in the digital age highlight risks such as widespread surveillance, discrimination, and the lack of effective remedies. In certain contexts, these approaches even recommend moratoriums on systems posing a high risk to rights until sufficient safeguards are in place. By comparison,

the AI Act adopts a legal approach of targeted bans and conditions, rather than a general moratorium, while explicitly acknowledging that some uses are "unacceptable" and must be prohibited. The difference becomes significant when applying exceptions: if international standards require very high thresholds of safeguards for intrusive technologies, an overly lax application of exceptions may create compatibility issues with obligations under the European Convention on Human Rights.

Conclusions

The AI Act represents a significant shift in EU law: a transition from appeals to ethics and self-regulation to a binding legal framework that explicitly treats fundamental rights as the object of protection in technology regulation. Its strengths include: (i) prohibitions on practices incompatible with dignity, autonomy, and non-discrimination; (ii) clear requirements for high-risk systems (risk management, data governance, transparency, and human oversight); (iii) the introduction of the FRIA, aligned with the DPIA under the GDPR; (iv) a core set of remedies (complaints and the right to explanations), supplemented by a sanctions regime; (v) EU-level governance mechanisms (the AI Council and the AI Office), relevant including for general-purpose AI models.

At the same time, three structural vulnerabilities can be identified. The first is selective coverage: the AI Act applies only to certain operators and certain systems, and the right to an explanation is conditional and "residual" relative to other rights under EU law. This may leave important areas of social life (including private activities with a diffuse impact) without sufficiently robust procedural tools. The second vulnerability is the tension between exceptions and oversight: in biometrics and law enforcement, the AI Act sets strict conditions, but experience from ECHR case law shows that technological intrusion without effective safeguards can have a chilling effect and erode public trust. The third is institutional capacity: enforcement through market oversight requires resources, expertise, and coordination; during the transition period (particularly until August 2, 2026, and, for some areas, until August 2, 2027), the quality of implementation will determine whether rights are protected in practice, not just on paper.

To strengthen compliance with international human rights obligations, two approaches are emerging. (a) The gradual expansion, through guidelines and administrative practices, of human rights impact assessments as a general due diligence practice, rather than merely a limited formal obligation. (b) Developing operational standards for transparency and accountability (audit, access to effective explanations and relevant documentation) that make procedural rights functional in real life, including in contexts of power asymmetries. In a landscape where the DSA, DMA, and data-related acts shape the information infrastructure of AI, the protection of human rights becomes a matter of systemic coherence, not merely of ad hoc compliance.

References

Charter of Fundamental Rights of the European Union. (2012). Official Journal of the European Union, C 326.

Council of Europe. (2024). *The Framework Convention on Artificial Intelligence* (CETS No. 225). https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

European Court of Human Rights. (2008*). S. and Marper v. the United Kingdom* (GC), Dec. 4, 2008.

European Court of Human Rights. (2021). *Big Brother Watch and Others v. the United Kingdom* (GC), May 25, 2021 (58170/13, 62322/14 and 24960/15).

European Court of Human Rights. (2023). *Glukhin v. Russia,* July 4, 2023.

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union, L 119.

Regulation (EU) 2022/1925 of the European Parliament and of the Council. (2022). Digital Markets Act (DMA). Official Journal of the European Union, L 265.

Regulation (EU) 2022/2065 of the European Parliament and of the Council. (2022). Digital Services Act (DSA). Official Journal of the European Union, L 277.

Regulation (EU) 2022/868 of the European Parliament and of the Council. (2022). Data Governance Act. Official Journal of the European Union, L 152.

Regulation (EU) 2023/2854 of the European Parliament and of the Council. (2023). Data Act. Official Journal of the European Union.

Regulation (EU) 2024/1689 of the European Parliament and of the Council. (2024). Artificial Intelligence Act. Official Journal of the European Union.

United Nations. (2011). *Guiding Principles on Business and Human Rights.* Implementing the United Nations "Protect, Respect and Remedy" Framework. Office of the High Commissioner for Human Rights. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

United Nations Committee on the Rights of the Child. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment.*

United Nations Educational, Scientific and Cultural Organization. (2021). *Recommendation on the ethics of artificial intelligence.* UNESCO.

United Nations Office of the High Commissioner for Human Rights. (2024). *The right to privacy in the digital age: The impact of artificial intelligence.* OHCHR.