

**PROTECTING HUMAN RIGHTS IN THE DIGITAL AGE IN LIGHT OF
THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE ACT: A
HUMAN-RIGHTS-BASED ANALYSIS OF THE RISK-BASED
REGULATORY MODEL**

Esra Özgün TEKIN

Ass. Prof., Kırıkkale University, Kırıkkale

email: esratekin@kku.edu.tr

Abstract

Technological advancements today have initiated a process of digital transformation that profoundly impacts social structures and individuals' positions within society. At the heart of this transformation lie artificial intelligence systems, which offer efficiency and innovation on one hand, while posing significant risks to fundamental human rights, privacy, and democratic values on the other. As algorithmic decision-making increasingly shapes individuals' rights and freedoms, serious questions arise about the adequacy of existing human rights regulation. The European Union's Artificial Intelligence Act (AI Act) is the first comprehensive legal framework aimed at regulating AI while protecting fundamental rights through a risk-based approach. Adopting a human-rights-based approach (HRBA) as its principal analytical lens, and drawing secondarily on theories of precautionary risk regulation and digital constitutionalism, this study examines the AI Act's risk-based model and analyses the threats of algorithmic discrimination, mass surveillance and democratic erosion that AI systems pose. The article further assesses the compatibility of the AI Act with the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, the Council of Europe Framework Convention on Artificial Intelligence, and the broader United Nations human rights framework, before evaluating whether the EU's regulatory influence is likely to generate a global standard through the so-called Brussels Effect. **Key words:** *EU AI Act, Fundamental Rights, Human Rights-Based Approach, International Human Rights Law, Risk-Based Regulation, Brussels Effect.*

1. Introduction

Artificial intelligence has emerged as one of the most significant regulatory challenges of the digital age. AI systems are no longer confined to experimental laboratories or narrowly technical environments; they are increasingly deployed in employment, education, healthcare, law enforcement, border management, financial services, public administration and digital communication. As a result, decisions that directly affect individuals' rights and opportunities are increasingly shaped by algorithmic systems rather than solely by human decision-makers, with profound implications for human rights, democratic governance and the rule of law.

The human rights dimension of artificial intelligence has attracted growing scholarly attention. The European Union has increasingly sought to develop a citizen-centred approach to AI regulation that prioritizes the protection of fundamental rights while supporting technological innovation (Marchenko & Entin, 2022). AI technologies increasingly influence democratic processes and may affect core rights such as freedom of expression, privacy, personal data protection and political participation (Kan, 2024), and their implications extend to freedom of assembly, access to information, equality, labour rights and voting rights (Gvaramadze, 2024). AI should therefore be understood not merely as a technological innovation but as a phenomenon capable of reshaping the practical enjoyment of fundamental rights.

The distinctive challenge posed by AI arises from its ability to generate decisions, recommendations and predictions through data-driven processes that are often difficult to explain or scrutinize. Unlike traditional software operating according to predetermined instructions, contemporary AI systems rely upon machine-learning techniques that identify patterns within large datasets and generate outputs through statistical inference, so that risks may emerge not only from deliberate human choices but also from biased datasets, algorithmic design choices and opaque decision-making structures (Kan, 2024).

Against this background, the European Union adopted Regulation (EU) 2024/1689, the Artificial Intelligence Act (AI Act) – the first comprehensive supranational legal framework governing artificial intelligence, built upon a risk-based regulatory model that seeks to promote trustworthy AI while protecting health, safety and fundamental rights (European Commission, n.d.). Rather than imposing uniform obligations on all AI systems, the Regulation differentiates between unacceptable, high, limited and minimal risks, reflecting the EU's broader attempt to reconcile technological innovation with human dignity (McCrudden, 2008), equality, democracy and the rule of law.

The significance of the AI Act extends beyond its role as an internal-market instrument: it is increasingly viewed as part of a broader European model of rights-based AI governance, reinforced by the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, which requires Parties to ensure that activities throughout the AI lifecycle remain consistent with human rights, democracy and the rule of law (Council of Europe, 2024). Together with the ECHR, the Charter of Fundamental Rights of the European Union and the

GDPR, the AI Act contributes to a multi-layered normative framework for governing artificial intelligence in Europe.

1.1. Theoretical Framework and Research Questions

This article situates its analysis within a human-rights-based approach (HRBA) to technology governance, which treats human rights not as an external constraint but as the organizing criterion against which a regulatory instrument's adequacy should be measured: whether it identifies rights-holders and duty-bearers, provides for transparency and accountability, and furnishes effective remedies (Wagner et al., 2022). This principal lens is supplemented by two secondary perspectives. First, risk-regulation theory cautions that precautionary intervention is defensible only where calibrated to the probability and severity of harm, since an undifferentiated precautionary stance can be paralysing rather than protective (Sunstein, 2005); the AI Act's four-tier risk taxonomy can be read as an attempt to avoid this indeterminacy while retaining anticipatory, rights-protective features such as the Fundamental Rights Impact Assessment. Second, digital constitutionalism situates the AI Act within a broader project of extending constitutional values – dignity, checks on algorithmic authority – into the digital sphere, explaining why the Act, although formally an internal-market measure, is increasingly read alongside the Charter and the ECHR as part of a constitutional settlement for algorithmic governance in Europe (De Gregorio, 2022).

Existing scholarship has examined either the human rights implications of AI or the regulatory architecture of the AI Act, but rarely their interaction with the Council of Europe AI Convention and broader international human rights law through an explicit HRBA lens. This article addresses that gap and, accordingly, asks: (i) to what extent does the AI Act's risk-based architecture operationalize the substantive and procedural requirements of a human-rights-based approach; (ii) how compatible are its safeguards with the ECHR, the Charter, the Council of Europe AI Convention and the UN human rights framework; and (iii) is the AI Act's model likely to generate extraterritorial convergence through the Brussels Effect, or is regulatory fragmentation the more probable outcome? The article proceeds in six further parts: the conceptual relationship between AI and human rights (Section 2); the principal human rights risks generated by AI (Section 3); the AI Act's risk-based architecture, mapped against those risks (Section 4); compatibility with the ECHR, the Charter, the Council of Europe Convention and the UN framework (Section 5); the Brussels Effect and comparative global governance (Section 6); and conclusions with policy implications (Section 7).

1.2. Methodology

This article adopts a qualitative doctrinal legal analysis combined with a comparative normative approach, applied through the HRBA framework above. Primary sources were selected for direct legal relevance (Regulation (EU) 2024/1689, the Council of Europe AI Convention, the ECHR, the Charter) and interpretive

relevance (UN Human Rights Committee materials, OHCHR reporting). Secondary literature was selected through a targeted review of law-and-technology scholarship published between 2016 and 2026, prioritising peer-reviewed journal articles and monographs on algorithmic accountability, explainability, non-discrimination and comparative AI governance.

The comparative dimension juxtaposes the AI Act's obligations with the ECHR, the Charter, the Council of Europe AI Convention and the ICCPR using a rights-by-rights method: for each right identified in Section 3 (privacy, equality, expression, democratic participation, effective remedy), the analysis asks what substantive standard the international instrument requires and whether a specific AI Act provision fully, partially, or does not operationalize it (summarised in Section 4.1). The analytical criteria are: (a) substantive coverage – whether a binding obligation, not merely a recital, addresses the right; (b) proceduralisation – whether an enforceable mechanism accompanies the obligation; and (c) accessibility of remedy – whether an affected individual has a realistic institutional pathway to challenge an AI-assisted decision. Because the methodology is normative rather than empirical, its conclusions describe what the AI Act's text requires in principle, not what providers and deployers will achieve in practice; statements regarding likely practical effectiveness – for example regarding the Brussels Effect or human oversight – are accordingly framed as plausible doctrinal expectations requiring future empirical verification.

2. Artificial Intelligence and Human Rights: Conceptual Framework

Artificial intelligence has fundamentally transformed the relationship between technology, law and society. Unlike traditional technological tools that merely facilitate human decision-making, AI systems increasingly participate in processes that directly affect individuals' rights, freedoms and opportunities, so that the regulation of AI cannot be reduced to technical governance alone. Viewed through the HRBA adopted here, AI governance is best understood as a question of whether rights-holders retain meaningful agency, transparency and recourse vis-à-vis increasingly autonomous decisional systems (Wagner et al., 2022).

One principal difficulty in regulating AI arises from the absence of a universally accepted definition of artificial intelligence; legal definitions must be sufficiently broad and technologically neutral to remain effective over time. The Council of Europe AI Convention defines an AI system as a machine-based system that, for explicit or implicit objectives, infers from its input how to generate outputs – predictions, recommendations, content or decisions – capable of influencing physical or virtual environments (Council of Europe, 2024). Regulation (EU) 2024/1689 similarly adopts a broad, functional definition under Article 3 (Regulation (EU) 2024/1689, Art. 3(1)).

The adoption of broad legal definitions reflects the recognition that AI's significance lies not merely in its technical architecture but in its societal consequences. Contemporary systems rely on machine-learning techniques that identify patterns and generate outputs through statistical inference, producing

decisions that are difficult to predict, explain or challenge – characteristics that distinguish AI from conventional software and create unique legal concerns relating to transparency, accountability and human oversight (Kan, 2024; Selbst & Barocas, 2018).

The relationship between AI and human rights is inherently multidimensional. AI-assisted medical systems may improve diagnoses and support the right to health; AI-driven educational technologies may facilitate access to learning; intelligent public-administration systems may enhance the delivery of public services. At the same time, the same technologies create substantial risks: human rights concerns extend beyond privacy and data protection to freedom of expression, assembly, access to information, equality, labour rights and democratic participation (Gvaramadze, 2024), and these risks intensify as AI becomes more deeply integrated into social and institutional structures.

A distinctive feature of AI governance is the multiplicity of actors involved in developing and deploying AI systems. Decisions are often the product of complex interactions between developers, providers, deployers and public authorities, so that responsibility for harmful outcomes may be fragmented, making it difficult for an affected individual to determine how a decision was reached or who bears legal responsibility (Florea, 2022; Kroll et al., 2017). These challenges demonstrate why AI governance cannot rely solely on voluntary ethical principles: effective regulation requires legally enforceable safeguards protecting human dignity, autonomy, equality, transparency and accountability (Leslie et al., 2021; Council of Europe, 2024). Digital constitutionalism situates this development within a longer trajectory in which constitutional values are extended into privately governed digital infrastructures, so that instruments such as the AI Act and the GDPR come to perform a quasi-constitutional function despite being formally ordinary legislation (De Gregorio, 2022).

Ultimately, artificial intelligence should be understood not merely as a technological innovation but as a regulatory challenge with profound implications for human rights protection. The central question is not whether AI should be permitted or prohibited, but how legal frameworks can maximize its social benefits while minimizing risks to individuals, democratic institutions and fundamental rights.

3. Human Rights Risks Generated by Artificial Intelligence Systems

The increasing deployment of AI across public and private sectors has generated significant concerns regarding its compatibility with fundamental rights protection. Unlike traditional technologies, AI systems can influence decision-making processes, shape social interactions and affect access to opportunities, resources and public services, so that their human rights implications must be examined within a broader legal and normative framework.

One of the most significant concerns relates to privacy and personal data protection. Contemporary AI systems depend on the collection, aggregation and

analysis of vast quantities of personal data; machine-learning models continuously process data to identify patterns and improve performance, facilitating forms of surveillance that remain largely invisible to individuals. The growing use of biometric identification, facial recognition and predictive analytics raises concerns regarding unauthorized data collection and the erosion of informational self-determination (Kan, 2024; Hoxhaj et al., 2023).

A second major challenge concerns algorithmic discrimination and inequality. Although AI systems are often perceived as objective, their outputs frequently depend on historical datasets containing embedded social biases. Foundational scholarship demonstrates that facially neutral data-mining processes can reproduce disparate impact along lines of race, gender and other protected characteristics, because the statistical correlations on which machine-learning systems rely are themselves the product of past discriminatory social practices (Barocas & Selbst, 2016). Machine-learning systems may thus reproduce or amplify inequalities affecting gender, ethnicity or socioeconomic status, particularly in employment, education, credit scoring and public services (Marchenko & Entin, 2022; Council of Europe, 2024; Barocas & Selbst, 2016), raising serious concerns for equality and non-discrimination and illustrating why formal neutrality in system design is an insufficient safeguard against substantive inequality.

AI systems also create challenges for freedom of expression and access to information. Algorithmic recommendation systems increasingly determine which information users encounter online; while this may improve efficiency, it may also shape public discourse by prioritizing certain viewpoints while marginalizing others, raising concerns for pluralism and democratic debate (Gvaramadze, 2024). Generative AI has further intensified concerns regarding misinformation, disinformation and the manipulation of public opinion.

The implications of AI for democracy are equally significant. Scholarship on online political micro-targeting demonstrates that profiling techniques developed for commercial advertising can be repurposed to tailor political messages to individual voters' psychological vulnerabilities, raising concerns about manipulation, a lack of transparency, and unequal access to the electorate (Zuiderveen Borgesius et al., 2018). The Council of Europe has recognized that AI may affect democratic institutions, political pluralism and judicial independence (Council of Europe, 2024), and concerns have emerged regarding behavioural manipulation and large-scale dissemination of misleading information, all of which may undermine democratic legitimacy and public trust.

Another critical challenge concerns transparency and explainability. Legal scholarship distinguishes inscrutability – the practical inability to inspect how a model functions – from non-intuitiveness – the difficulty of understanding why a model's outputs are what they are even where its logic can be inspected; regulatory demands for 'explainable' machines will fail to secure genuine accountability unless they address both properties, including the normative justification for a model's design choices (Selbst & Barocas, 2018). Individuals may thus be unable to understand why

a decision was reached or how it may be challenged, undermining procedural fairness (Hoxhaj et al., 2023; Selbst & Barocas, 2018).

Closely related is accountability. Traditional legal systems assume decisions can be attributed to identifiable human actors, but in AI environments responsibility is distributed among developers, providers, deployers and public authorities, complicating the attribution of liability (Florea, 2022). Accountability scholarship argues that technical mechanisms – audit trails, procedural regularity, disclosure of design criteria – must supplement or substitute for full transparency, particularly where disclosing source code would itself compromise privacy or security (Kroll et al., 2017), directly relevant to assessing the AI Act's documentation obligations. A further complication concerns human oversight itself: comparative empirical research on human-in-the-loop policies across many jurisdictions finds that human reviewers are frequently unable to meaningfully detect or correct algorithmic errors, so that a formal oversight requirement can create a false sense of security rather than genuinely constraining automated decision-making (Green, 2022), a critique directly relevant to Article 14 of the AI Act (Section 4).

Finally, AI systems may affect the right to an effective remedy and access to justice. Automated decision-making may reduce opportunities for meaningful human review, limiting the ability of affected persons to contest adverse outcomes; without adequate transparency and oversight, legal remedies risk becoming theoretical rather than practical (Council of Europe, 2024). Taken together, these risks demonstrate that AI has the potential to affect virtually every dimension of fundamental rights protection, providing the background against which the EU adopted the AI Act.

4. The EU AI Act and the Risk-Based Regulatory Approach

The AI Act represents the most comprehensive regulatory attempt to govern artificial intelligence through a structured, rights-oriented framework. Rather than regulating all AI systems uniformly, it adopts a risk-based approach reflecting the principle of proportionality (Alexy, 2002), seeking to balance technological innovation with the protection of fundamental rights, health, safety and democratic values (Marchenko & Entin, 2022). Read through risk-regulation theory, the model can be understood as a deliberate departure from an undifferentiated precautionary stance, calibrating the intensity of intervention to the probability and severity of rights-related harm (Sunstein, 2005).

The AI Act establishes four broad risk categories – unacceptable, high, limited and minimal (European Commission, n.d.; Marchenko & Entin, 2022) – so that compliance requirements remain proportionate to potential impact. Article 5 prohibits AI practices considered fundamentally incompatible with European values, including manipulation of behaviour, exploitation of vulnerabilities, certain social scoring and specific biometric identification uses (Regulation (EU) 2024/1689, Art. 5), reflecting a normative commitment to human dignity and democratic society regardless of potential economic benefits.

The core of the AI Act is the regulation of high-risk AI systems. Under Article 6 and Annex III, systems used in employment, education, essential services, law enforcement, migration management and the administration of justice may be classified as high risk (Regulation (EU) 2024/1689, Art. 6, Annex III), given that decisions in these sectors often have substantial life consequences. Providers of high-risk systems are subject to obligations relating to risk management, data governance, technical documentation, record-keeping, transparency, accuracy and cybersecurity (Regulation (EU) 2024/1689, Arts. 9–15), reflecting a lifecycle approach in which compliance is a continuous process – a logic that corresponds closely to accountability scholarship's insistence that documentation and audit trails, rather than source-code transparency alone, render an algorithmic system reviewable over time (Kroll et al., 2017).

A key safeguard is human oversight: Article 14 requires high-risk systems to be designed to enable effective oversight by natural persons (Regulation (EU) 2024/1689, Art. 14), ensuring significant decisions remain subject to meaningful human judgment. This safeguard should not, however, be assumed to function automatically: comparative evidence indicates that human reviewers frequently lack the time, expertise or institutional incentive to meaningfully second-guess an algorithm's recommendation, and oversight requirements can paradoxically legitimize deployment of systems whose reliability has not been independently established (Green, 2022). This does not negate Article 14's value, but suggests its efficacy depends on implementing guidance specifying reviewer competence and workload conditions rather than a formal requirement of human presence alone.

The Act further strengthens rights protection through Fundamental Rights Impact Assessments (FRIAs): Article 27 requires certain deployers of high-risk systems to evaluate foreseeable impacts on fundamental rights before deployment (Regulation (EU) 2024/1689, Art. 27), reflecting an increasingly preventive approach that seeks to mitigate risks before they materialize rather than relying exclusively on ex post remedies.

Despite these strengths, the risk-based model faces criticism: risk classification may itself be uncertain and contested, and providers may have incentives to classify systems in ways that minimize obligations, potentially under-regulating harmful technologies (Marchenko & Entin, 2022). Enforcement is a further challenge, since effectiveness depends on the capacity of supervisory authorities to monitor compliance; without robust enforcement, well-designed safeguards may fail to provide effective protection. Because this article's methodology is doctrinal rather than empirical, these concerns are presented as plausible risks flagged by the regulatory design, pending future empirical verification as the Regulation's obligations progressively enter into application.

4.1. Mapping Human Rights Risks to AI Act Safeguards

Table 1 summarises how each risk identified in Section 3 is addressed – fully, partially, or not at all – by a specific AI Act safeguard, applying the analytical criteria

of substantive coverage, proceduralisation and accessibility of remedy set out in Section 1.2.

Fundamental Right at Risk	Principal Risk Mechanism	Corresponding AI Act Safeguard(s)
Privacy and data protection	Mass biometric surveillance; opaque profiling	Art. 5 prohibitions; data-governance duties (Art. 10); FRIA (Art. 27)
Equality / non-discrimination	Biased training data reproduced in employment, credit, education	High-risk classification (Art. 6, Annex III); bias-testing duties (Art. 10)
Freedom of expression / information	Algorithmic curation; generative-AI disinformation	Transparency obligations (Art. 50); synthetic-content labelling
Democratic participation	Micro-targeted political communication; voter manipulation	Art. 5 prohibition of manipulative techniques; FRIA
Effective remedy / access to justice	Fragmented responsibility; limited explainability	Right to explanation (Art. 86); complaint mechanisms

Table 1. Mapping of principal human rights risks to corresponding AI Act safeguards

Coverage is strongest where a risk maps onto a concrete, individually enforceable provision, such as the Article 5 prohibitions or the Article 86 right to explanation, and comparatively weaker where the safeguard is procedural rather than substantive, as with the FRIA requirement, whose rights-protective value depends heavily on implementation quality. This distinction between formally complete and substantively effective protection recurs throughout Section 5.

5. Compatibility with International Human Rights Standards

The AI Act should not be assessed in isolation from the broader framework of European and international human rights law. Although formally adopted as an internal-market measure, its substantive provisions demonstrate a clear commitment to fundamental rights protection and must be interpreted within a normative architecture including the ECHR, the Charter, the GDPR and the Council of Europe AI Convention. The following subsections examine each layer in turn.

5.1. The European Convention on Human Rights

The ECHR provides a foundational framework for rights that may be affected by AI, including respect for private and family life (Art. 8), freedom of expression (Art. 10), freedom of assembly (Art. 11), non-discrimination (Art. 14) and the right to a fair trial (Art. 6). These guarantees run closely parallel to the privacy, expression and non-discrimination provisions of the ICCPR (Arts. 17, 19, 2 and 26), so that the European and UN layers of protection substantially reinforce one another rather than operating in isolation (United Nations, 1966); the distinct enforcement architecture of each system is addressed in Section 5.4.

The increasing use of algorithmic decision-making in public administration, law enforcement and judicial contexts demonstrates that AI may influence both substantive and procedural dimensions of Convention rights. Applying the criteria above, the AI Act's coverage of Article 8 concerns is comparatively strong, given the Article 5 prohibitions on biometric surveillance; its coverage of Article 6 fair-trial concerns is weaker, since the Regulation does not itself create judicial review mechanisms and instead relies on national procedural law.

5.2. The Charter of Fundamental Rights of the European Union

The Charter further strengthens this framework, expressly recognizing the right to data protection (Art. 8) and providing guarantees concerning human dignity (Art. 1), equality (Arts. 20–21), effective remedies (Art. 47) and good administration (Art. 41). Because the AI Act operates within the EU legal order, it must be interpreted consistently with Charter rights (Hoxhaj et al., 2023), functioning as a constitutional benchmark consistent with the digital-constitutionalism account of quasi-constitutional legislative instruments (De Gregorio, 2022). The UN Human Rights Committee's interpretation of equivalent ICCPR guarantees offers a further interpretive resource for Charter rights that lack a settled ECHR analogue, most notably the standalone data-protection guarantee of Article 8 (United Nations, 1966).

Coverage of Articles 8 and 21 is generally strong, given the data-governance and bias-testing obligations discussed in Section 4; coverage of Article 47's right to an effective remedy is more limited, since the Regulation's remedial provisions (Art. 86) apply only to certain high-risk decisions and otherwise defer to national procedure.

5.3. The Council of Europe Framework Convention on Artificial Intelligence

The Council of Europe AI Convention provides a broader normative framework grounded in human rights, democracy and the rule of law, requiring Parties to ensure AI-lifecycle activities remain consistent with these values (Council of Europe, 2024). Its relationship with the AI Act is complementary: the Act establishes concrete mechanisms, while the Convention articulates broader interpretive principles (Council of Europe, 2024; Rotenberg, 2025). Convergence is visible in the shared emphasis on transparency as a precondition for accountability, on equality and non-discrimination (Council of Europe, 2024; Marchenko & Entin, 2022; Barocas & Selbst, 2016), and

on human oversight – although, as noted in Section 4, the doctrinal existence of an oversight requirement should be distinguished from its practical efficacy (Green, 2022). The right to an effective remedy is a further point of convergence, though questions remain regarding whether individuals will obtain meaningful explanations in practice (Selbst & Barocas, 2018).

Despite these developments, compatibility should not be assumed automatically: much depends on implementation, enforcement and judicial interpretation. Nevertheless, the AI Act represents an important attempt to translate abstract human rights principles into concrete obligations, and, read alongside the ECHR, the Charter and the Council of Europe Convention, can be understood as part of an emerging human-rights-based framework for AI governance in Europe.

5.4. The United Nations Human Rights Framework

Beyond the European architecture, compatibility with UN instruments warrants consideration. The ICCPR protects rights directly implicated by AI deployment, including privacy (Art. 17), freedom of expression (Art. 19) and non-discrimination (Arts. 2, 26) (United Nations, 1966). The UN High Commissioner for Human Rights has called for a moratorium on AI systems posing serious risks absent adequate safeguards, and has highlighted that algorithmic decision-making may violate privacy where deployed without transparency, necessity and proportionality constraints (OHCHR, 2021). The AI Act's biometric-surveillance prohibitions and transparency requirements are broadly consistent with these standards, though enforcement mechanisms and the scope of prohibited practices differ considerably (Gvaramadze, 2024; Leslie et al., 2021). Assessing the Act against this backdrop reveals both ambition and limitation: it operationalizes key human rights principles within a binding structure, but does not constitute a comprehensive implementation of all international human rights obligations relating to AI.

Taken together, Sections 5.1–5.4 point to three residual regulatory gaps that persist despite the AI Act's evident achievements. First, a fair-trial and judicial-review gap: the Act creates no dedicated mechanism for challenging an AI-assisted decision before a court, leaving Article 6 ECHR and Article 47 Charter concerns to be resolved by uneven national procedural law. Second, an enforcement-uniformity gap: because supervisory capacity varies across Member States, formally identical obligations may translate into materially different levels of protection in practice – a limitation the Act shares with the Council of Europe Convention and, more broadly, with the ICCPR's reliance on domestic implementation.

Third, a scope gap vis-à-vis the UN framework: the Act's rights guarantees are calibrated to EU constitutional values and do not purport to operationalize the full range of ICCPR obligations, so that individuals outside the Act's territorial and material scope remain dependent on the weaker enforcement architecture of international human rights law. These gaps do not undermine the overall assessment that the AI Act constitutes a significant step towards human-rights-based AI

governance, but they mark the precise points at which future legislative or judicial development is most needed.

6. The Brussels Effect and Global AI Governance

The significance of the AI Act extends beyond EU borders. As with the GDPR, it possesses the potential to influence regulatory developments globally through the “Brussels Effect” (Bradford, 2020) – the EU’s ability to externalize its standards due to market size, the attractiveness of European market access, and the costs of maintaining different compliance regimes.

AI developers and multinational corporations seeking access to the European market are likely to adapt their governance structures to AI Act requirements, since maintaining separate systems for different jurisdictions may be economically inefficient. The final text of Regulation (EU) 2024/1689 reinforces this by extending obligations to providers and deployers outside the Union where AI systems or their outputs are used within the European market (Regulation (EU) 2024/1689, Art. 2). However, this influence should not be assumed automatic. Bradford’s comparative analysis situates the AI Act within a contest among three regulatory models for the digital economy – the market-driven American model, the state-driven Chinese model, and the rights-driven European model – each actively exported through trade relationships and platform compliance decisions (Bradford, 2023).

A systematic comparative survey confirms considerable divergence persists: the United States relies on a largely non-binding, sectoral federal approach supplemented by state legislation; China has adopted binding but narrowly targeted rules embedded within a state-led governance system; and the United Kingdom prefers a principles-based, regulator-led model without a single horizontal statute (Hilliard et al., 2026).

Canada’s experience illustrates a further, distinct pattern: its proposed Artificial Intelligence and Data Act, which would have introduced a risk-based framework broadly modelled on the AI Act, died on the order paper when Parliament was prorogued in January 2025 and has not been reintroduced, leaving federal AI governance to a patchwork of privacy law, provincial statutes such as Quebec’s Law 25, and sectoral directives (Chambers and Partners, 2026). This outcome is a reminder that regulatory fragmentation may result as much from domestic political contingency as from principled disagreement over regulatory philosophy. It is therefore important to distinguish genuine regulatory harmonization from mere voluntary corporate compliance, whereby a provider adopts AI Act-consistent practices as internal risk management without any change in the binding law of the jurisdictions where it operates (Hilliard et al., 2026; Bradford, 2023).

Nevertheless, the European approach possesses distinctive normative appeal, integrating innovation with human rights protection, democratic governance and the rule of law, offering an alternative to the largely unrestricted American model and the state-centred Chinese model (Bradford, 2023). Bradford’s original analysis identifies

four structural conditions enabling the Brussels Effect – market size, regulatory capacity, inelastic targets and non-divisibility of standards (Bradford, 2020) – all of which the AI Act appears well-positioned to satisfy, as demonstrated by the GDPR precedent and by several technology companies already announcing global implementation of AI Act-inspired risk classification (Rotenberg, 2025). Consistent with the methodological caveat above, however, whether these voluntary adaptations represent genuine normative convergence or minimum-threshold commercial compliance remains an open empirical question (Bradford, 2023; Hilliard et al., 2026).

The most significant contribution of the European model may therefore lie not in establishing universal legal rules but in shaping global expectations regarding responsible AI governance – even as, in sectors where the American or Chinese models retain a decisive commercial or geopolitical advantage, regulatory fragmentation rather than convergence may persist (Hilliard et al., 2026).

7. Conclusion

Artificial intelligence has emerged as one of the most significant technological and regulatory challenges of the contemporary era. While AI systems offer substantial opportunities for innovation and improved public services, they also create significant risks for fundamental rights, democratic governance and the rule of law, so that AI governance is no longer merely a technical issue but a matter of legal and societal importance.

Applying the HRBA set out in the Introduction, this article has argued that the AI Act should be understood not simply as an internal-market instrument but as a central component of an emerging human-rights-based model of AI governance. By adopting a risk-based approach calibrated against precautionary risk-regulation theory, the AI Act seeks to reconcile innovation with fundamental rights protection, and the mapping in Section 4.1 demonstrates that this translation is, on balance, substantively strong for privacy- and equality-related risks and comparatively weaker for risks to democratic participation and effective remedy. The analysis further demonstrated that the AI Act operates within a multi-layered normative framework – the ECHR, the Charter, the GDPR and the Council of Europe Convention – well captured by the digital-constitutionalism literature's account of quasi-constitutional ordering in the algorithmic society (De Gregorio, 2022).

At the same time, the study identified challenges affecting the AI Act's effectiveness. Difficulties relating to risk classification, transparency, accountability and enforcement may limit its capacity to protect fundamental rights in practice; comparative evidence on human oversight in other contexts suggests a formal oversight obligation is not, by itself, a guarantee of meaningful human control (Green, 2022). Consequently, the AI Act's long-term success will depend not only on the quality of its legal framework but on effective implementation, robust institutional oversight and meaningful access to justice.

Despite the challenges identified, the AI Act represents a significant step towards trustworthy, human-centric artificial intelligence, demonstrating that technological innovation and human rights protection need not be competing objectives. Future research should focus on the practical implementation of the AI Act – particularly the effectiveness of Fundamental Rights Impact Assessments, transparency obligations and human oversight mechanisms – employing empirical methods that lie beyond the doctrinal scope of the present article but are indispensable for testing the normative expectations it has articulated. Ultimately, the success of the AI Act will be measured not by the sophistication of its regulatory categories but by its ability to ensure that individuals can understand, challenge and obtain remedies for decisions that affect their rights and lives.

7.1. Policy Implications

Several policy implications follow. First, implementing guidance should prioritise sector-specific classification criteria for high-ambiguity domains such as generative AI in public administration, given the gap between the Act's formally comprehensive taxonomy and practical classification uncertainty. Second, the Article 14 human oversight requirement should be operationalized through binding standards specifying reviewer competence and caseload limits, addressing the false-security risk identified in comparative literature (Green, 2022). Third, given the gap between Charter Article 47 and AI Act Article 86, Member States should consider clarifying the procedural pathway for challenging high-risk AI-assisted decisions before national courts. Fourth, supervisory authorities and the EU AI Office should invest in the capacity necessary for meaningful enforcement, since doctrinal adequacy does not by itself guarantee practical efficacy. Fifth, the implications of the AI Act for EU candidate countries deserve dedicated attention, since accession negotiations are likely to generate *de facto* pressure to transpose AI Act-equivalent obligations well before formal membership; a related but distinct question concerns non-EU states that are not seeking accession but may nonetheless pursue voluntary regulatory alignment with European standards – whether through EEA/EFTA-style market-access arrangements, bilateral trade agreements, or, as Canada's experience in Section 6 illustrates, the simple absence of a comparably developed domestic alternative – a dynamic that merits comparative study in its own right.

References

- Alexy, R. (2002). *A theory of constitutional rights* (J. Rivers, Trans.). Oxford University Press.
- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671–732.
- Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
- Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.
- Chambers and Partners. (2026). Artificial intelligence 2026 – Canada: Trends and developments. Chambers and Partners Global Practice Guides. <https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2026/canada/trends-and-developments>
- Council of Europe. (2024). Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Council of Europe Treaty Series No. 225). Council of Europe.
- De Gregorio, G. (2022). *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society*. Cambridge University Press.
- European Commission. (n.d.). AI Act. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- European Parliament and Council. (2024). 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). Official Journal of the European Union, L 2024/1689, 12 July 2024.
- Florea, A. M. (2022). Artificial intelligence & human rights in the European Union. *Law Review [Revista de Drept]*, 12(Special Issue), 80–90.
- Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, 45, 105681. <https://doi.org/10.1016/j.clsr.2022.105681>
- Gvaramadze, T. (2024). Human rights and artificial intelligence. *Journal of Law (TSU)*, 2024(2), 124–139.
- Hilliard, A., Gulley, A., Kazim, E., & Koshiyama, A. S. (2026). Artificial intelligence policy worldwide: A comparative analysis. *Royal Society Open Science*, 13(2), 242234. <https://doi.org/10.1098/rsos.242234>
- Hoxhaj, O., Halilaj, B., & Harizi, A. (2023). Ethical implications and human rights violations in the age of artificial intelligence. *Balkan Social Science Review*, 22, 153–170.
- Kan, C. H. (2024). Artificial intelligence (AI) in the age of democracy and human rights: Normative challenges and regulatory perspectives. *International Journal of Eurasian Education and Culture*, 9(25), 145–166. <http://dx.doi.org/10.35826/ijoecc.1825>

- Kroll, J. A., Huey, J., Barocas, S., Felten, E., Reidenberg, J., Robinson, D., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*, 165(3), 633–705.
- Leslie, D., Burr, C., Aitken, M., Cowls, J., Katell, M., & Briggs, M. (2021). Artificial intelligence, human rights, democracy, and the rule of law: A primer. Council of Europe.
- Marchenko, A. Y., & Entin, M. L. (2022). Artificial intelligence and human rights: What is the EU's approach? *Digital Law Journal*, 3(3), 43–57. <https://doi.org/10.38044/2686-9136-2022-3-3-43-57>
- McCrudden, C. (2008). Human dignity and judicial interpretation of human rights. *European Journal of International Law*, 19(4), 655–724. <https://doi.org/10.1093/ejil/chn043>
- OHCHR [Office of the United Nations High Commissioner for Human Rights]. (2021). The right to privacy in the digital age (A/HRC/48/31). United Nations Human Rights Council. <https://undocs.org/en/A/HRC/48/31>
- Rotenberg, M. (2025). Introductory note to Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Council of Europe). *International Legal Materials*, 64, 859–902.
- Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. *Fordham Law Review*, 87(3), 1085–1139.
- Sunstein, C. R. (2005). *Laws of fear: Beyond the precautionary principle*. Cambridge University Press.
- United Nations. (1966). International Covenant on Civil and Political Rights. United Nations Treaty Series, 999, 171. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- Wagner, B., Kettemann, M. C., Vieth-Ditlmann, K., & Montgomery, S. (Eds.). (2022). *Research handbook on human rights and digital technology* (2nd ed.). Edward Elgar Publishing.
- Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodó, B., & de Vreese, C. H. (2018). Online political microtargeting: Promises and threats for democracy. *Utrecht Law Review*, 14(1), 82–96. <https://doi.org/10.18352/ulr.420>