International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS)

International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS Journal) | ISSN (e): 2808-4713
Volumes 5 No. 6 (2025)

Impact and Legal Challenges of Artificial Intelligence Violating Human Rights: A Socio-Legal Study

Mohd Aamir Malik[1]
LL.M Scholar, Department of Law, CT University, Ludhiana, Punjab, India
Corresponding Author's email address: advmalikaamir@gmail.com

Received	: 15 November 2025	Published	: 22 January 2026
Revised	: 01 December 2025	DOI	: https://doi.org/ 1.54443/ijebas.v5i6.5040
Accepted	: 30 December 2025	Link Publish	: https://radjapublika.com/index.php/IJEBAS

Abstract

Artificial intelligence (AI) technologies have experienced a massive developmental process and have created unheard opportunities in several industries. But it has created a major alert related to plundering of basic human rights as well. Anthony M and Anthony have highlighted some of the issues with AI as bias in algorithms that endangers fair trial and equality, mass surveillance that imposes on privacy and freedom of expression. This socio-legal research examines the way the development of AI affects the protection of human rights and how the law in various states aces the challenge of addressing AI-generated rights infringements. Based on the concept of international human rights and the new jurisprudence, the research demonstrates an accountability, transparency and ethical protection regulation gap. It ends with a call to promote a humanistic vision of the law that would put innovation in line with respect of rights.

Keywords: Artificial intelligence, human rights, algorithmic bias, legal accountability, digital rights, socio-legal analysis

Introduction

Artificial intelligence (AI) has become an extraordinary phenomenon that is reformulating world economies, social, and jurisprudential patterns. Its acceptance in both the public and the private sectors has contributed to some brilliant changes in the aspect of automation, data processing, and predictive analysis. Whether that is financial services and healthcare, education, and law enforcement, AI-driven systems have already become part of the daily decision-making process. Although the technologies are beneficial in increasing operational efficiency and providing solutions to complicated issues, they elicit deep-rooted and many faceted menace to basic human rights. Algorithmic decision-making has crept into surveillance, predictive policing, job seeking, welfare recipients, and facial recognition, and opens up such grave issues as discrimination, violation of privacy, data mining, and undermining the guarantees of due process issues (Crawford, 2021). These are not only technical matters but profoundly socio-legal and touch upon the matters of power, governance and responsibility. As an example, when training AI algorithms on historical records with unrepaired biases, they will promote those inequities, impacting disadvantaged populations more gravely. On the same note to black box and inexplicable models of decision making, fundamental legal values of transparency, fairness, the right to a remedy are called into question. The use of AI when it comes to surveillance and profiling tools further enhanced the concerns over state-based oppression and big-scale exploitation of data, diminishing the civil liberties and principles of democracy. The paper describes how AI technologies affect human rights and critically discusses the legal and regulatory threats connected to their implementation. Taking a more socio-legal approach, it studies the role unregulated or poorly regulated autonomous AI has in creating structural injustice, enhancing social exclusion, and straining legal doctrines. The paper assesses the sensitivity of the existing legal frameworks such as domestic regulations, laws and international instruments on human rights to AI violations. It also locates unaddressed accountability-related gaps and gives policy recommendations toward enhancing the human-centric and the rights-respecting governance of AI. The end-line of the paper is that the law should be ready to meet the new technological environment without prejudicing human dignity, liberty, and equality even in an era dominated by artificial intelligence.

AI and the Violation of Human Rights

Algorithmic Bias and Discrimination

Artificial intelligence is neutral to the extent of the information that it is trained on. Even when machine learning algorithms are seen to be objective or objective-like, they tend to reproduce a large percentage of existing social bias in historical data. When AI models are used to learn representations of some societal aspect that lacks equality, e.g. discriminatory policing records, biased hiring histories or gender-biased financial data, they replicate these representations across a large representation scale. It leads to so-called digital poorhouse (Eubanks, 2018), in which inequality is institutionalized via automated systems under the banner of efficiency and neutrality. One of these strong cases can be seen in facial recognition technology, which has been proven to have remarkably higher error rates among women and people of color to the point where it should be questioned whether it is racially and sexually discriminatory. Buolamwini and Gebru (2018) discovered that the commercial facial analysis algorithms had been most effective with light-skinned male faces and least efficient with dark-skinned female faces. Such differences would be in direct violation of the right to equality and non-discrimination, enshrined in Article 7 of the Universal Declaration of Human Rights (UDHR, 1948) and Article 2 of the International Covenant on Civil and Political Rights (ICCPR).

An AI-based decision-making process has been associated with discriminatory outcomes in employment, credit scores, insurance, and housing that violate economic and social rights, such as the right to work, equality of opportunity and the right to adequate standard of living. In one recent instance, algorithmic screening tools utilized during the hiring process have been found to prefer the candidates of the male gender over a women of equal or greater qualifications as it was based on biased training data, skewed by a fact that the workforce has mostly been male-dominated historically. In the same sense, predictive policing, which uses AI, has also become under fire due to its tendency to target people of color disproportionately. Police departments that use past arrest data inevitably focus more on patrols and attention to the areas that already face over-policing. Not only does this reinforce the racial profiling impulse, but it also entails a breach in the right to liberty and security of a person, provided in Article 9 of the ICCPR. What is more, the practice leads to a spiral of structural injustices, as the communities, which suffer its consequences, are further marginalized through systems that should maintain order and safety within society. In any case, the discriminative effects of AI are not incidental consequences but symbols of intensive structural discrimination. Legal systems need to then transition to proactive and not reactive forms of governance, whereby developers and deployers of the AI system are obligated to undertake algorithmic impact analysis, data representativeness and more practical human oversight. In the absence of such safeguards, AI technologies are bound to put forward and institutionalize, the very inequalities the human rights law aims at eradicating.

Mass Surveillance and the Right to Privacy

Facial recognition, biometric tracking, geolocation camera monitoring and the mining of large amounts of data using AI has allowed mass surveillance on an unprecedented scale by both state and non-state actors. Such technologies, which are also frequently used under the banners of national security or civil tranquility, are far too easily used to operate in the grey areas of the law, with little to no oversight or accountability. In that way, they present a critical danger to the privacy right, which is stipulated in Article 12 of the Universal Declaration of Human Rights (UDHR, 1948) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR, 1966). Authoritarian governments have now become more weaponized using AI-powered surveillance to enforce political opposition, social authorities and inhibit any form of dissent. The facial recognition technologies are used by governments to monitor protestors, block content online, and there is the usage of the so-called social credit systems, which result in punishments of being outside of state practices. These kinds of practices not only infringe on the right to privacy, but also on freedom of expression, the right to assemble, as well as the political participation, which are key principles of democratic regimes (Feldstein, 2019). The chilling effect that has been exerted by following the people always suppresses the work of the civil society and undermines the principle of democratic accountability. In even democratic countries, an uneasiness is increasingly developing with the growth of what Zuboff (2019) refers to as surveillance capitalism, i.e., the commodification and monetizing of personal data by IT firms without any significant user agreement. AI-based technologies retrieve behavioral data using smart phones, smart devices and online and their terms of service are usually hidden and not clear. These issues of trading human experience are highly ethical and legal questions of human autonomy, informed consent, and human dignity. In these situations, user becomes not only a consumer but is reduced to datafied body, with the preferences, habits and identities being forecasted, manipulated and commoditized with no proper protection or redress.

Furthermore, the overlapping between state surveillance and the gathering of data about citizens by corporations increases the cost of infringing on the rights. Joint activities, i.e., joint activities of the state and the commercial enterprise, in predictive policing or health data analysis may be used to obtain information about one subject or stratify another one, without prior notice to its users or mandatory limitations of the purpose similar to boundaries related to the ownership of data. Without strict legal forms and architecture that protects privacy, AI-based surveillance systems can operate to disembowel constitutional guarantees as well as widen vertical disparities. The socio-legal problem will not, then, be only to uncover cases of excess, but rather to fashion rights-based governance arrangements that govern surveillance through their transparency, much less the necessity and proportionality, and accountability. This entails the enactment of restrictions on facial recognition applications, requiring a regulatory use review of surveillance technologies, and enhancing laws that safeguard datapossession (data protection) to enable the informational self-determination of people across jurisdictions.

Due Process and Accountability Gaps

Application of AI in sensitive areas like immigration control, welfare distribution and criminal justice admits grave issues of due procedure and procedural fairness. The working of these algorithmic systems is frequently in a non-transparent or un-understandable form by those who are most likely to be affected by it. Such tendency is also known as the so-called problem of the black box, involving the fact that the logic of machine learning models is opaque, leaving the decision-making process unavailable to end users as well as to those who develop it as well as regulators of it (Wachter, Mittelstadt, & Floridi, 2017). This, in turn, may also lead to the denial of visas, social benefits, or even freedom with no explanations of the decisions and no chance to appeal them or make some objections.This is directly contrary to a legal protection which is core to the perspective of human rights, comprising the right to a fair trial, the right to an effective remedy and the presumption of innocence (International Covenant on Civil and Political Rights [ICCPR], 1966, Articles 14 and 2). AI has been used more in predictive policing, sentencing, and risk assessment tools in criminal justice systems. Nevertheless, these systems can be based on biased data and erroneously predict the amount of risk or can overestimate the risk of recidivism a choice that can discriminate against underrepresented groups and unwarrantedly incarcerate or deny the opportunity to post bail (Angwin et al., 2016).

Additionally, failure to establish accountability systems of AI-caused harm compounds the quest of justice. These are constructed on the basis of human actions and will, whereas the AI systems act independently, the question of who or what can be held answerable in the case of rights violation. Is it the developers who coded the system, the deployers who used it as a decision making tool, or the data providers who contributed to making it, whose fault is it? The lack of uniformity in assigning responsibility in law leaves a gap in the area of tort, administrative and criminal liability rendering victims with no proper legal remedy (Pagallo, 2013). Such lack of accountability is particularly severe when it comes to administrative choices in the area of immigration or welfare. As an example, welfare fraud detection algorithmic systems have falsely accused someone who actually qualifies to receive welfare benefits leading to denial of such benefits or even legal sanctions without the opportunity to appeal or be verified. The dearth of algorithmic visibility and explainability becomes a challenge in making any appeal, more so to vulnerable people who might lack the luxury of legal assistance and technology literacy. To combat those difficulties, a consensus can be seen on legal obligations to AI systems where it is being widely accepted that it is necessary to introduce components of legal obligations, such as the right to explanation, algorithmic auditing, and liability measures. The rights-based system of AI governance should provide that decisions that interfere with fundamental rights of people should not be devoid of human check and legal scrutiny as well as democratic supervision. In the absence of such protections, the efficiency and scalability provided by AI can be at the unacceptable cost of justice, transparency and human dignity.

Legal and Regulatory Challenges

Fragmented Legal Landscape

Although the international human rights law provides a universal normative background, with a focus on dignity, equality, privacy and due processes, the law on control over artificial intelligence (AI) is rather decentralized and varied in different jurisdictions. As an illustration, the United Nations Guiding Principles on Business and Human Rights (UNGPs) specify that both states and corporations have obligations to avoid the violation of rights associated with technological practice. These principles are however non binding and the way that they have been adopted in the nations has not been stable and proactive but instead, reactive (United Nations, 2011).

Among regional efforts, the **European Union's AI Act (2021)** stands out as the most comprehensive and systematic attempt to regulate AI. It introduces a **risk-based classification** of AI systems—categorizing them as unacceptable, high-risk, limited-risk, or minimal-risk—and imposes strict requirements for transparency, accountability, and fundamental rights protection on high-risk systems (European Commission, 2021). Notably, applications like biometric surveillance, predictive policing, and algorithmic hiring fall under the high-risk category, necessitating **human oversight, impact assessments, and clear documentation**. This rights-conscious approach reflects the EU's broader digital strategy and its alignment with the **Charter of Fundamental Rights of the European Union**. In contrast, the **United States** has taken a more **sectoral and decentralized approach**, relying on voluntary frameworks and industry self-regulation. AI governance tends to be **domain-specific**—for example, handled separately by bodies like the Federal Trade Commission (FTC) in consumer protection or the Food and Drug Administration (FDA) in medical AI. While various bills have been introduced in Congress, such as the **Algorithmic Accountability Act (2022)**, there is still **no unified federal AI law**, and most regulatory guidance remains **non-binding** or advisory in nature. This results in **inconsistent protections**, especially for vulnerable populations who may be affected by discriminatory algorithms or opaque surveillance technologies (Calo, 2021). Other countries have taken varied routes. An example of such is the rapid increase in AI usage in such areas as surveillance and social governance in China, as well as the release of guidelines like the Internet Information Service Algorithm Recommendation Management Provisions (2022), which pay more attention to regulating content and security, rather than human rights. At the same time, India does not have an AI-specific law yet; however, it seems to be actively working on digital governance, including the introduction of new laws, such as Digital Personal Data Protection Act (2023), which are, regardless, controversial in terms of their enforcement means and compatibility with human rights (Singh, 2023). Such regulatory discrepancy will result in a gap at the global governance level, which will make enforcing cross-border responsibility, data sovereignty, and universality of AI safety and rights difficult. There is a danger that due to the lack of international coordination and binding processes, unequal protection of rights and the ability of corporations to engage in forum shopping would further fuel the problem of global inequality and digital injustice.

Lack of Legal Personhood for AI

One of the most pressing legal challenges in regulating artificial intelligence lies in the **question of accountability**: who is responsible when AI systems cause harm or violate human rights? Although AI systems can act autonomously—making decisions without direct human intervention—they are **not recognized as legal persons** under current legal systems. This lack of legal personhood creates **significant challenges in assigning liability**, especially when decisions made by algorithms result in discrimination, privacy breaches, or other rights violations (Pagallo, 2013). Traditional legal doctrines, particularly in **tort law and criminal liability**, are premised on the assumption of a **human or corporate actor with agency and intent**. Legal responsibility typically requires establishing fault, foreseeability, and a causal link between the action and the harm. However, **autonomous AI systems**, especially those that evolve through unsupervised learning, may act in ways that are not fully predictable by their developers or users. This results in a scenario where **no single party may be directly culpable**, even though harm has clearly occurred.

The diffusion of responsibility in AI ecosystems further complicates the matter. AI systems are the product of **multiple stakeholders**—data providers, developers, algorithmic trainers, deployers, and end users—each playing a role in shaping the system's behavior. Determining **who should be held accountable** when the system produces biased outcomes or infringes on rights becomes a legal grey area. Should the liability fall on the **software engineer**, the **company that deploys the AI**, or the **government agency** that uses the system in public services? The absence of clear legal attribution undermines **remedial justice**, leaving victims without a clear path for redress (Pagallo, 2013; Yeung, 2018). Some scholars and policymakers have proposed introducing **electronic personality** for advanced AI agents—granting them a limited legal status to enable liability attribution and insurance frameworks (European Parliament, 2017). However, this approach is controversial. Critics claim that it shifts blame off human beings against the greater corporate responsibility and suggests legal fictions how they cannot have adequate oversight, and instead, regulation should be enforced (Bryson, 2018). It is precisely the existing gap in regulation that requires the emergence of a body of AI-specific laws that would address both the specificities of machine autonomy and strengthen human-centred frameworks of responsibility. The existing recommendations are the introduction of a strict liability framework, joint liability frameworks, or the establishment of mandatory impact assessments on AI with traceability. Until these structures are put

in place the disparity between technological invention and technological responsibility shall keep on increasing- with as severe implications as to human rights action and to the moral acceptability of the law.

Jurisdiction, Data Sovereignty, and Transnational Enforcement Challenges

The tendency towards the integration of artificial intelligence (AI) systems into the digital infrastructure of this world is such that these systems nowadays regularly work across national borders and use and store personal data in any jurisdiction. This transnational aspect to the implementation of AI results in a complicated panoply of lawfare associated with data citizenship, jurisdiction, and enforcement of human rights. Specifically, it is not always clear what legal regime governs when an AI-powered rights infringement appears, on which side of the law the question is to be addressed, and how the corrective measures may be implemented in case AI-driven rights violation takes place. One of the most critical areas that have to be addressed is data sovereignty, the right to the control of the data created on a territory of the nation-state. With cloud computing and AI applications hosted by multinational corporations, user data is often transferred and processed in data centers located in other countries—sometimes with vastly different legal standards on privacy, accountability, and redress. This **geographical decoupling** of data from jurisdiction weakens the ability of affected individuals or states to assert their rights or demand legal remedies under domestic laws (Greenleaf, 2018).

Consider a scenario in which a person in India is profiled or denied services by an algorithm trained and operated by a company based in the United States, using data stored on servers in Ireland. In such a case, **what court has the authority to hear the claim? Which national law applies? How can a judgment be enforced across borders?** These are not hypothetical concerns but increasingly common realities, especially in AI applications involving **social media algorithms, online credit scoring, automated content moderation**, and **facial recognition systems** (De Gregorio, 2021). Current **international legal frameworks** offer limited answers. While instruments like the **General Data Protection Regulation (GDPR)** in the European Union attempt to extend protections extraterritorially, their efficacy depends on **political will, reciprocal agreements**, and the **existence of enforcement mechanisms**. Many developing countries still lack comprehensive data protection laws or institutional capacity to enforce cross-border claims. Furthermore, **international human rights law**—although theoretically universal—is often **unenforceable in private sector contexts**, particularly when violations occur through non-state actors like tech corporations (UN Human Rights Council, 2021). Efforts to establish **international cooperation mechanisms**, such as through **mutual legal assistance treaties (MLATs)** or regional digital compacts, remain fragmented and underdeveloped. In absence of obligatory and unified transnational legal frameworks, corporations can resort to so-called forum shopping by setting the location of the operation in jurisdiction with lax oversight policies to evade responsibility. This gives rise to what the legal scholars refer to as a regulatory arbitrage landscape where the protection of the rights is compromised by law fragmentation (Bradshaw et al., 2010). Multilateral approach is required to deal with such issues. This would involve drafting of binding international standards on algorithmic accountability, aligning data protection laws and developing international enforcement mechanisms across borders. Furthermore, by incorporating AI regulation into international human rights system, e.g., at the UN or regional judicial courts, it would be possible to fill the jurisdictional gap, which leaves victims of cross-border AI harm without redress.

Socio-Legal Implications

As a matter of the social fact, however, utilization of artificial intelligence (AI) technologies frequently imitates and enhances the current structural disparities as opposed to eradicating these. Instead of being impartial or generally useful, AI systems often capture the stakeholders, societies, politics, and economies, in which they work. These technologies have been instilled with the notions, biases, and blind-spots of the people who created the technologies, which are normally elite national North-based developers, and the damages lie on the vulnerable and marginalized groups (Benjamin, 2019). As another example, predictive policing, welfare eligibility decisions, hiring, and loan approvals made by AI-powered tools can be trained using racist, sexist, casteist, or classist patterns of historical data that reflect the past discrimination. As a result, such systems uphold biased results further paving the way to inequalities that the law claims to be handling. According to the words of Eubanks, (2018), machines targeting efficiency in delivering welfare services frequently turn into the digital poorhouse as low-income communities are subjected to aggressive monitoring and are deprived of goods and services due to opaque algorithms. This means that AI does not only mirrors systemic exclusion but entrenches it institutionally.

Instead of acting as a disciplinary measure, the legal system can hardly follow the speed of technological changes. Such regulation in lag permits the powerful firms in AI development and deployment to do so with little to no government regulation allowed under the pretext of innovation. Tech conglomerates control regulation by asking to have light-handed self-regulation on the one hand and putting soft-pedal on ethical issues, portraying them as technical challenges that can be overcome through design, not structural change. This technocratic reasoning paves the way of overriding the issue of human rights and pushing the concerned communities even further on the sidelines of the policymaking process (Yeung, 2018). Moreover, the mistiness and accountability of AI systems undermine the public confidence in both technology and the legal systems. The right to have access to justice is destroyed when people have to deal with the effect of a decision made based on an algorithm that they cannot unravel or challenge. Not only does this distance people from the law, but it also worsens what the literature in law refers to as the democratic deficit, which is the exercise of power with little input by the citizens, little control, and little redress (Zuboff, 2019). The proposed socio-legal issues demand that regulatory perspectives be adjusted on a progressive level. We need an inclusive, rights-based, and intersectional framework of AI governance in which voices of historically disadvantaged communities are prioritized and access to technology, privacy, redress, and other such issues are understood as social justice, and not as a compliance issue. Implementing such transparency, participation, and accountability in the design and control of AI systems and making the law work to serve not only as a tool of reactive responses but also as an active protection of human dignity and equality.

Recommendations

This should be considered in view of the multidimensional socio-legal issues presented by artificial intelligence (AI) to the basic human rights and therefore a multidimensional regulation is necessary. The recommendations provided below help in eliminating the gap of introducing technological innovations and rights-based governance:

1. **Adopt Human Rights Impact Assessments (HRIAs) for High-Risk AI Systems**
   It is on the governments and organizations to demand that all systems or AI that fall in the category of high-risk applications should be provided with a pre-deployment Human Rights Impact Assessment, particularly where the application can be in policing practices, welfare, border management, or employment. Such examinations should examine possible damage to the right to privacy, avoidance of discrimination, due process, and dignity and consultations with affected groups. Incorporation of HRIAs during procurement and designs would be a step to aligning AI practices with the UN Guiding Principles on Business and Human Rights (UNGPs, 2011) and propagation of anticipatory governance.
2. **Mandate Algorithmic Transparency and the Right to Explanation**
   Laws have to ensure that there is transparency of algorithms and a statutory right to explanation on any automation decision that is highly prejudicial to the rights of people. This entails the availability of reasonable information regarding the decision making process; data involved and criteria employed. These would be procedurally fair and in line with such instruments as Article 8 of the European Convention on Human Rights and Article 14 of the ICCPR.
3. **Establish International AI Governance Bodies**
   The fragmented nature of AI regulation across jurisdictions necessitates the creation of a **multilateral AI governance framework**, possibly under the auspices of the **United Nations**, **OECD**, or a newly created **Global AI Rights Commission**. This body would be tasked with setting baseline norms, monitoring compliance with international human rights standards, facilitating cooperation, and adjudicating cross-border complaints. Such a mechanism would help mitigate the **accountability gap** in transnational data practices.
4. **Implement Enforceable Accountability and Liability Frameworks**
   National legislatures should introduce **clear liability regimes** that allocate responsibility among developers, deployers, and users of AI. This entails the strict or vicarious liability during the violation of rights due to an automated decision and the obligatory insurance programs of a provider of AI. Such frameworks will help operationalize redress mechanisms and deter negligence in AI design and deployment (Pagallo, 2013).
5. **Promote Digital Literacy and Inclusive Policymaking**
   The future of AI that respects rights needs an extensive digital literacy program to enable citizens, including members of marginalized groups, to learn and challenge AI systems that impact them. Moreover, the agenda of inclusive AI governance must establish the requirement of public consultations, a participatory evaluation of

technology, and auditing conducted by the community to make policymaking processes democratic and discourage AI policymaking monopolization by corporate or technocratic elites (Benjamin, 2019).

Conclusion

Artificial intelligence (AI) is a potentially transformational technology that can be used to advance the welfare of people, promote better service delivery, and curb the emergence of social problems. Notwithstanding, such a promise is coupled with immense threats to core human rights, particularly where AI technologies are advanced and applied without proper legal and ethical regulations. This socio-legal inquiry has demonstrated the way in which AI is not neutral since it can create and replicate power disparities that exacerbate discrimination, breach privacy and undermine due process. Existing (national and international) regulatory environments are piecemeal, reactive and poorly adapted to address the problems that are inherent to autonomous, opaque and transnational AI systems. The inability to establish clear mechanisms of accountability and the nonexistence of enforceable safeguards to the vulnerable people presents a potential threat to technological innovation and legal justice. The solution to overcome the danger of this gap includes the necessity of the comprehensive and rights-based AI governance approach that should be based on human dignity, equity, and democratic accountability. This will need something more than technical solutions and ethics codes of self-help. It requires legal structures that create enforceable obligations to algorithmic transparency and require assessments by the human eye, legal duty of care, and a designation of statutory responsibility, including the notion of including marginalized people in the decision-making process. In the end, the path ahead to harmonize the disconnect between innovation and justice will entail a paradigm shift: one in which a market-based AI agenda is transformed into an ethics-based and socio-legal accountability one. As AI is increasingly used to define the future of societies, it is only a regulatory requirement that principles of human rights should be incorporated into its design and implementation processes, but rather a moral one.

References

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim Code*. Polity Press.

Bradshaw, S., Millard, C., & Walden, I. (2010). Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services. *International Journal of Law and Information Technology, 19*(3), 187–223. https://doi.org/10.1093/ijlit/eaq011

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Proceedings of Machine Learning Research* (Vol. 81, pp. 1–15). https://proceedings.mlr.press/v81/buolamwini18a.html

Calo, R. (2021). Artificial intelligence policy in the United States: The need for a coordinated approach. *Brookings Institution*. https://www.brookings.edu/articles/artificial-intelligence-policy-in-the-united-states/

Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.

De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law, 19*(1), 41–70. https://doi.org/10.1093/icon/moab001

European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Feldstein, S. (2019). The global expansion of AI surveillance. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Privacy Laws & Business International Report*, (145), 10–13.

Pagallo, U. (2013). *The laws of robots: Crimes, contracts, and torts*. Springer.

United Nations. (1948). *Universal Declaration of Human Rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations Human Rights Council. (2021). *The right to privacy in the digital age* (A/HRC/48/31). https://undocs.org/A/HRC/48/31

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI for robotics. *Science Robotics, 2*(6), eaap6962. https://doi.org/10.1126/scirobotics.aap6962

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance, 12*(4), 505–523. https://doi.org/10.1111/rego.12160

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