



Lex Gazette International Multidisciplinary
Research Journal

DOUBLE BLIND PEER REVIEWED

 OPEN ACCESS

REGULATING ALGORITHMIC AUTHORITY: AN INTERDISCIPLINARY LEGAL STRUCTURE OF ARTIFICIAL INTELLIGENCE RESPONSIBILITY

Harini S

Student at the Alliance School of Law, Bangalore

Contact at: harinisakkra2005@gmail.com

ABSTRACT

Artificial intelligence (AI) has become a rapidly growing topic not only of technical devices but also a powerful socio-legal agent, which shapes governance, markets, the health of people, environmental laws, media reports, and even individual rights. Once algorithms have handled an increasing number of the decisions that have been historically left to the discretion of humans, then the existing legal frameworks struggle to hold any of them responsible, just, and valid. The paper employs an interdisciplinary approach of law when explaining how the law ought to respond to AI-enabled change in the field of technology regulation, data privacy, and public policy, as well as economics, sociological, psychological, and international regulation. It asserts that the multi-dimensional impacts of AI could not be regulated using traditional, socio-legal models and proposes the implementation of a comprehensive system of accountability within the context of the constitutional values and ethical governance, and sustainable development. The article introduces a normative concept to the future-ready legal regulation as the ability to balance innovation and justice through putting the AI within the frames of a more structured social organization and regulatory ecosystems

KEYWORDS

Artificial Intelligence, Algorithmic Accountability, Data Privacy, Multidisciplinary Law, Legal Ethics, Governance

I. INTRODUCTION

The development of increasing the use of artificial intelligence in decision-making systems is one of the most radical changes currently influencing modern society. The functions of producing the state-market-person relationships are more and more mediated by algorithmic technologies, and the functions previously under the jurisdiction of human discretion. Predictive policing and credit scores, medical diagnostics and climate modelling are just a few examples of AI-powered systems that have much more legal and social implications.¹ Although artificial intelligence is touted as a device of efficiency, neutrality, and objectivity, its application has also increased the threats of opacities, discrimination, marginalisation, and unaccountable power concentration.² The normative system of law, which has the role of organising society and protecting rights, is therefore confronted with a basic problem: how do legal systems change in response to non-human decision-makers that are increasingly defining the lives of humans?

Historically, legal tradition has been constructed along the lines of identifiable human agents, linear causation, and harms that have a geographical location. Liability regimes, constitutional protection and protection of the procedure presuppose intent, explanation and jurisdiction. These assumptions are shaken by artificial intelligence. Distribution Distributed across intricate networks of developers, deployers, and users across multiple jurisdictions, algorithmic decision-making is not necessarily deterministic but probabilistic, not transparent, and opaque.³ These features strain the traditional dogmas governing liability, responsibility, and the enforcement of rights, making it hard to find proper blame, proportionality, or effective solutions.⁴

The regulatory issue of AI is not limited to the technology law field. Instead, it permeates various spheres of legislation, including the environmental law, where the algorithms determine how resources should be managed and the climate rules; the public health, where AI will determine the diagnoses and policy-making; the market law, where automatic systems will affect the competition and consumer behaviour; the gender justice, where biased information

¹ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3–6 (Harvard Univ. Press 2015).

² Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* 11–14 (St. Martin's Press 2018).

³ Karen Yeung, Algorithmic Regulation: A Critical Interrogation, 12 Reg. & Governance 505, 508–10 (2018).

⁴ Danielle Keats Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249, 1254–56 (2008).

can enforce structural inequality; the criminal law, where predictive technology will shape the liberty and due process; education, where automated systems are redefining learning and assessment; the international relations, where cross-border technologies will challenge the jurisdictional and sovereign boundaries.⁵ The broad nature of AI signifies the ineffectiveness of the regulations that are silo-based.

In this paper, the author believes that the meaningful regulation of artificial intelligence cannot take place without a multidisciplinary legal analysis combining the experience of technology studies, economics, sociology, psychology, ethics, and political science. Instead of treating AI as a neutral technical artefact, law has to appreciate it as a socio-technical system that is employed in the power relations, institutional practices, and normative choices.⁶ In line with this, the present paper reviews the legal regulatory implications of AI in key fields of law and proposes an accountability-oriented framework that can ensure management of the cross-sectoral and global repercussions of algorithmic decision-making. The paper aims to leave a trace in the creation of a future-proof legal architecture that considers both innovation and justice by basing AI governance on the principles of constitutional values, human dignity, and democratic legitimacy.

2. LEGAL, TECHNOLOGICAL, AND ALGORITHMIC RESPONSIBILITY.

The core issue of the regulation of artificial intelligence is the aspect of accountability of algorithms. Algorithms are being assigned the tasks increasingly with a direct and substantial impact on the legal rights, such as access to welfare, determining the risk of bail and sentencing, the distribution of state funds, and the postponement of speech on online platforms.⁷ Even as their power is increasing, most AI systems are black boxes, not subject to examination due to technical complexity, proprietary design, or purported trade secrets.⁸ Such a lack of transparency conditions the contrary effect on key rule-of-law principles of transparency, reasoned decision-making, and entitlement to be heard, without which the legitimacy of legal and administrative action is impossible.⁹

⁵ Shoshana Zuboff, *The Age of Surveillance Capitalism* 94–97 (PublicAffairs 2019).

⁶ Julie E. Cohen, Law for the Platform Economy, 51 U.C. Davis L. Rev. 133, 137–40 (2017).

⁷ Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* 37–40 (St. Martin's Press 2018).

⁸ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3–5 (Harvard Univ. Press 2015).

⁹ A.K. Kraipak v. Union of India, (1969) 2 SCC 262 (India).

The ability to recognise, review and impose penalties upon the individuals who caused injuries that were caused by algorithmic systems. It demands that the processes of decision-making should be interpretable, challengeable and subject to significant supervision. Nevertheless, the current legal processes have partial solutions. The administrative law review, as an example, has long been interested in judicial review of the human discretion exercised by government officials as opposed to non-human products produced by complex and proprietary machine processes.¹⁰ As long as the decision-making powers of the standard, that is, reasonableness, proportionality, and procedural fairness, are not reduced to adequate delegation to the algorithms, they are difficult to adopt in practice.

Correspondingly, the tort law and product liability regimes find it difficult to fit the special features of self-learning and adaptive AI systems. The product liability models are usually developed to deal with the manufacturing defects or the design flaws that could be identified during the manufacturing process. On the other hand, harm in machine-learning systems can be found in dynamical processes, and there does not seem to be a causal relationship with an existing design error.¹¹ This diffusion of responsibility of developers, deployers, data providers and users generates accountability deficiencies which permit both public and private actors to avoid liability through attributing harm to technological complexity.

To address the challenges, risk-based AI governance models are becoming more and more popular among new regulatory frameworks. These frameworks identify the AI systems according to their potential harm and high-risk applications, specifically those in the sphere of public administration, law enforcement and critical infrastructure, are more likely to become more supervised.¹² Such requirements may involve compulsory human supervision, algorithmic effect tests, documentation and post-implementation surveillance. Although risk-based regulation is a considerable improvement, it cannot be effective on its own.

Risk-based strategies should be accompanied by effective procedural controls in order to achieve a true sense of accountability. The rights to explanation, access to reasons, and opportunities to appeal algorithmic decisions should be granted to the affected individuals.¹³

¹⁰ Jerry L. Mashaw, Reasoned Administration: The European Union, the United States, and the Project of Democratic Governance, 76 Geo. Wash. L. Rev. 99, 104–07 (2007).

¹¹ Mark A. Lemley & Bryan Casey, Remedies for Robots, 86 U. Chi. L. Rev. 1311, 1318–22 (2019).

¹² Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), arts. 6–9.

¹³ Danielle Keats Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249, 1301–06 (2008).

In the absence of these protections, oversight will be reduced to a mere formality or symbol, providing compliance, but no justice. Finally, algorithmic accountability should be incorporated into the current legal traditions, but should also be adjusted to the new reality of automated decision-making so that the exercise of algorithmic power does not contradict constitutional values and the rule of law.¹⁴

3. SURVEILLANCE CAPITALISM, DATA PRIVACY, AND CYBERSECURITY

The systems of artificial intelligence cannot be achieved without significant extraction, aggregation, and analysis of data on a large scale. This data-centric model has spawned what scholars term as surveillance capitalism, whereby personal data is commoditised to make predictions, shape, and commercialise human behaviour.¹⁵ In these kinds of ecosystems, people are frequently turned into information points, and informational asymmetries allow states and corporations to gain control over social and economic life as never before. Therefore, the law of data protection has taken a leading role in the regulation of AI.

Purpose limitation, data minimisation, informed consent, and proportionality are some of the principles that are used in constructing modern data protection regimes.¹⁶ These pillars have the purpose of limiting the unregulated data mining and the fact that informational authority should not override personal freedom. Nonetheless, AI systems make these securities more complex, as it allows secondary and unintended applications of data, making inferences more intrusive than the original data.¹⁷ Predictive analytics, behavioural modelling, and biometric identification represent how AI can invade privacy without being outright data collection.

The cybersecurity vulnerabilities also increase these threats. The breach of big and sensitive data, including health, financial, and governmental data, incurs a high risk, which raises a significant question of state and corporate responsibility.¹⁸ Constitutionally speaking, informational privacy cannot be broken down into ideas of dignity, autonomy, and freedom of expression. The fact that privacy is recognised in the judicial system as a right is indicative of increasing fear that unrestricted surveillance kills democratic action and the oppression of

¹⁴ UNESCO, *Recommendation on the Ethics of Artificial Intelligence* 18–21 (2021).

¹⁵ Shoshana Zuboff, *The Age of Surveillance Capitalism* 8–10 (PublicAffairs 2019).

¹⁶ Regulation (EU) 2016/679, General Data Protection Regulation, arts. 5–6.

¹⁷ Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 Seton Hall L. Rev. 995, 1002–05 (2017).

¹⁸ Paul Ohm, Broken Promises of Privacy, 57 UCLA L. Rev. 1701, 1725–28 (2010).

dissenting opinions.¹⁹ The proper regulation of AI need should, thus, to combine the data protection legislation, cybersecurity regulations, and the human rights ideals into a single system that will limit both governmental and corporate surveillance.

4. ARTIFICIAL INTELLIGENCE, POPULATION HEALTH, AND BIOETHICAL REGULATION

The application of AI in medical care and government health management proves the radical potential of automated decision-making as well as the inherent ethical dangers of its existence. In reaction to the pandemic, AI-based systems were used in contact tracing, predictive modelling, and resource allocation, and regularly increased the efficiency of administration and responsiveness.²⁰ Simultaneously, these technologies also brought up grave issues of consent, discrimination, transparency and proportionality, especially when utilised in emergencies.

Mental health AI-driven applications also create problems with regulatory oversight. The systems are often based on granular behaviour information and probabilistic evaluation of mental states. Without effective protective measures, they are prone to misdiagnosis, stigmatisation, and misuse, with vulnerable populations being disproportionately affected.²¹ The bioethical principles, such as autonomy, beneficence, non-maleficence, and justice, therefore, gain greater importance when it comes to regulating AI-assisted healthcare.

The law is an important factor in making ethical norms binding in the form of an obligation. Regulations should also make sure that medical decisions made with the help of AI can be explained by professionals, who should be accountable, and at the same time, consider the rights of patients.²² The technological precision of health systems is not enough to ensure the proper level of public trust, but legal legitimacy, transparency and the promise that the human judgment is central to the care provision.

¹⁹ K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

²⁰ World Health Org., *Ethics and Governance of Artificial Intelligence for Health* 12–15 (2021).

²¹ I. Glenn Cohen et al., *The Promise and Perils of AI in Mental Health*, 393 *Lancet* 1079, 1080–82 (2019).

²² Jacob Metcalf et al., *Algorithmic Impact Assessments and Accountability*, 43 *Colum. J.L. & Soc. Probs.* 1, 18–22 (2020).

5. MARKETS, CORPORATE GOVERNANCE, AND ECONOMIC REGULATION

Artificial intelligence has changed the market structure with high-frequency trading, algorithmic pricing, automated consumer profiling, and data-driven competition strategies. On the one hand, these innovations should guarantee efficiency and expansion; on the other hand, there is a threat of manipulating the market, non-inclusive practices, and tacit collusion.²³ The competition law is challenged with new threats when algorithms are coordinating the outcome in ways that do not explicitly require human consensus, and are challenging the fundamental principles of antitrust.

Corporate governance systems should evolve to make AI implementation compliant with the fiduciary obligations, risks, and social responsibility. Due diligence, transparency, and liability are some of the questions that pop up as algorithms are increasingly informed or replacing managerial decision-making. The directors can not exonerate themselves by blaming the poor performance on the technological systems.²⁴ The legal responsibility should be tied to human control and institutionalisation.

Economically, AI regulation should strike the right balance between the incentives of innovation and consumer protection and distributive justice. Algorithms' power is currently being concentrated in a handful of large companies, which may lead to the establishment of monopolies and the strengthening of disparities. The law should hence encourage the existence of competitive markets, deter the abuse of dominance, and ensure that the AI benefits are fairly shared.²⁵

6. ALGORITHMS, SOCIOLOGY, GENDER, AND STRUCTURAL BIAS

The artificial intelligence systems tend to reproduce and amplify the current social disparities due to the fact that they are being trained on biased data sets that are historically based. Such technologies as facial recognition have shown increased error rates in women, racial minorities, and marginalised groups, which poses a serious issue for the constitutional equality and non-

²³ Ariel Ezrachi & Maurice E. Stucke, *Virtual Competition* 45–49 (Harvard Univ. Press 2016).

²⁴ Andrew D. Selbst, *Regulating AI as Corporate Governance*, 43 *Yale J. on Regul.* 1, 14–19 (2022).

²⁵ Lina M. Khan, *Amazon's Antitrust Paradox*, 126 *Yale L.J.* 710, 780–85 (2017).

discrimination standards.²⁶ These disparities show the fallacy of the algorithmic impartiality and bring out the social inertia of technological orders.

The algorithmic bias is not merely a technical imperfection, but according to a socio-legal analysis, it is an injustice that has a structural nature. Law should thus go beyond formal equality and adopt substantive equality, which deals with the condition of the system that yields biased results.²⁷ Such harms can be solved by tools such as algorithmic impact assessment, inclusive data governance, and participatory design, but only with the help of the provision of enforceable legal norms.

The gender justice models have been found to be especially important when determining the effect of AI on the job market, access to credit, welfare allocation, and government service. Patriarchal norms and exclusionary practices are likely to be supported by AI without any conscious effort.²⁸ The Law should also serve as a rectifying measure, not an eroding factor of social justice, because the technical evolution should develop alongside the legislation.

7. MEDIA, MISINFORMATION AND DEMOCRATIC DISCOURSE.

Digital platforms with the help of artificial intelligence are now the key arenas in the development and spread of the opinion of the masses. Such sites are no longer the passive hosts of the speech but actively shape the visibility of the information, its reach, and framing using the algorithmic curation, ranking, recommendation systems, and so on. Through content filtering, emphasising the engagement-based stories, and regulating speech at scale, AI systems gradually become the regulators of the digital common space by themselves.²⁹ Although these technologies have opened access to information and facilitated quick communication, they have also increased the dissemination of untrue information and deep fakes, as well as ideologically insulated echo chambers.³⁰ This directly involves the core constitutional values of freedom of speech, democratic participation and the right to information, which is why AI-driven media regulation has them directly in its sights.³¹

²⁶ Joy Buolamwini & Timnit Gebru, Gender Shades, 81 Proc. Mach. Learning Res. 1, 7–10 (2018).

²⁷ Sandra Fredman, *Substantive Equality Revisited* 34–38 (Oxford Univ. Press 2016).

²⁸ UN Women, *Gender Equality and Artificial Intelligence* 6–9 (2020).

²⁹ Jack M. Balkin, Free Speech in the Algorithmic Society, 51 U.C. Davis L. Rev. 1149, 1153–55 (2018).

³⁰ Shoshana Zuboff, *The Age of Surveillance Capitalism* 187–89 (PublicAffairs 2019).

³¹ Romesh Thappar v. State of Madras, AIR 1950 SC 124 (India).

Algorithms are a structural risk to a democratic discourse because of misinformation heightened by the algorithmic systems. Interestingly, AI-based recommendation engines tend to give priority to the content that can best attract the users (maximising user engagement), and this can favour sensational, polarising or emotionally charged content, neglecting the factual content that is accurate and balanced.³² This risk is also worsened by the Deepfake technologies, which erase the boundary between reality and fiction and affect how society trusts the media organisations and the election process.³³ When the citizens are not able to differentiate between trustworthy information and the content that has been manipulated, the deliberative principles of democracy are undermined, and informed political engagement becomes more challenging.

Meanwhile, content moderation is directly problematic in terms of censorship and an a priori limitation of speech. Artificial intelligence moderation systems are often not as transparent as they can be, and they can have a disproportionate impact on marginalised voices, political dissent, or minority voices.³⁴ Malfunctioning automated moderation, like excessive blocking of legitimate speech or failure to block harmful speech, shows the weakness of algorithmic judgment as the only tool that should govern areas that need normative and contextual judgment. The privatisation of ensuring speech regulation, in turn, to the platforms, which are controlled by unintelligible algorithms and business regulations, thus overturning the common ideas of what state responsibility and constitutional responsibility mean.³⁵

The primary legal issue is whether the responsibility of the platforms can be reconciled with the freedom of speech. There is a danger of over-regulation of online environments by the state, where the regulation will suffocate expression and create a potential totalitarian control over the online space, and, conversely, the Internet will abound in harmful content that corrupts the discourse of democracy.³⁶ To find this balance, the legal solution to this issue must be sophisticated and based on the fact that platforms wield considerable power in society, but should not be turned into censorship tools.

³² Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* 76–79 (Yale Univ. Press 2018).

³³ Bobby Chesney & Danielle Citron, Deepfakes and the New Disinformation War, 66 Foreign Aff. 147, 150–52 (2019).

³⁴ Danielle Keats Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249, 1301–05 (2008).

³⁵ Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

³⁶ Tim Wu, Is the First Amendment Obsolete?, 117 Mich. L. Rev. 547, 559–62 (2018).

An AI-driven media regulatory regime, which is respectful of rights, must thus focus on transparency, procedural fairness, and an independent regulator. The platforms must make available the logic and the criteria that guide the content moderation and recommendation systems, especially when these systems deal with political speech or information that has a public interest. Procedural protection measures (notice, explanation, and appeals) are necessary so that the users have avenues to meaningfully contest the decisions of content moderators.³⁷ In addition, an independent regulatory force may be important to monitor the practices of the platform, establish minimum criteria of accountability, and avoid arbitrary or discriminatory execution.

The bottom line of the issue of democratic rhetoric in the era of artificial intelligence is whether or not the law can be used to control the power of algorithms without compromising the liberties that it aims to safeguard. Instead of regarding AI-driven media as neutral intermediaries, the legal frameworks need to recognise them as effective actors of the public sphere. Law can facilitate the enforcement of constitutional principles, human rights principles and democratic accountability in the regulation of media to ensure that artificial intelligence becomes a source of strength, and not a source of erosion, to the circumstances that are essential to an informed and participatory democracy.³⁸

8. CRIMINAL JUSTICE, PSYCHOLOGY, AND REHABILITATION.

The increased application of artificial intelligence in criminal justice systems, especially predictive policing, sentencing, and risk assessment, provokes deep-seated questions of fairness, due process, and presumption of innocence. There has been an increased use of algorithmic tools to predict criminal behaviour, estimate the probability of reoffending, and influence the decisions of bail, sentencing, and parole. As much as these technologies are commonly vindicated in terms of efficiency and objectivity, their implementation reveals structural contradictions between the predictability of data and the postulates of criminal law.³⁹

Predictive policing tools are based on historical crime data, and this data is often a remnant of a system of over-policing in a marginalised area. Consequently, algorithmic predictions have a

³⁷ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), arts. 14–17.

³⁸ UNESCO, *Recommendation on the Ethics of Artificial Intelligence* 22–27 (2021).

³⁹ Bernard E. Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age* 17–19 (Univ. of Chi. Press 2007).

risk of strengthening already found biases as opposed to neutralising them.⁴⁰ Psychological studies go even further to show that the results of algorithms can have a dramatic impact on the process of judicial and law enforcement decision-making, and that these results in what is commonly referred to as an automation bias. Officials and judges can abide by an algorithmic recommendation even where such a recommendation is inconsistent with the surrounding evidence or fairness.⁴¹ This kind of deference can generate feedback processes where biased data will give rise to biased predictions supporting more surveillance and punitive processes, hence perpetuating systemic injustice.⁴²

The use of the probabilistic assessment of risk, as viewed through the lens of constitutional and human rights, is a significant challenge to due process. The traditional basis of criminal liability has been individual responsibility and demonstrated behaviour as opposed to statistical probability and risk profile on a group basis.⁴³ The application of algorithmic risk scores poses the danger of changing the criminal justice system so that it does not penalise past offences but proactively anticipates future risks, which breaks the principle of proportionality and the presumption of innocence.⁴⁴ When the people are treated worse because they are likely to do something when they are not proven to be guilty, then the very justice system becomes challenged.

The use of predictive technologies is a particular threat to rehabilitation-oriented justice systems. Criminal law is not just punitive but corrective in nature, which seeks to reintegrate criminals into society. The reliance on the algorithmic tools can destroy the significance of such aspects of the rehabilitation as empathy, moral reasoning, and individualised judgment, which are crucial to the process of meaningful rehabilitation.⁴⁵ When applied as a matter of authority and not as an advisor, risk assessment tools may shrink individuals, dehumanising them and thereby removing the human element that demands that justice is served.

The law should thus guarantee that artificial intelligence is applicable only as an addition to, and not a replacement of, human judgment when it comes to criminal justice decision-making.

⁴⁰ Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 Ga. L. Rev. 109, 124–29 (2017).

⁴¹ Karen Yeung, *Algorithmic Regulation: A Critical Interrogation*, 12 Reg. & Governance 505, 512–14 (2018).

⁴² Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016).

⁴³ State of Punjab v. Baldev Singh, (1999) 6 SCC 172 (India).

⁴⁴ Sonja B. Starr, Evidence-Based Sentencing and the Scientific Rationalization of Discrimination, 66 Stan. L. Rev. 803, 806–10 (2014).

⁴⁵ Nicola Lacey, *The Prisoners' Dilemma: Political Economy and Punishment in Contemporary Democracies* 45–47 (Cambridge Univ. Press 2008).

Some transparent legal principles are required in order to regulate the admissibility, transparency, and contestability of the algorithmic evidence. The defendants should be entitled to the right to know and dispute the application of an algorithmic judgment that impacts their freedom.⁴⁶ Courts should always be held to great accountability as long as their decision-making is based on the constitutional values, ethical judgment, and compassion as opposed to the enigmatic technological determinism.⁴⁷

9. ETHICS, EDUCATION AND FUTURE OF LEGAL PEDAGOGY.

The changing effect of artificial intelligence in legal training is being felt in the introduction of automated legal research, predictive models and artificial intelligence-based assessment instruments. The use of such technologies has led to efficiency and transparency in the access to legal information that can be searched within plenty of cases and legislation in a short period of time.⁴⁸ Nevertheless, the increasing adoption of artificial intelligence tools in learning is raising multiple ethical and moral questions in regard to integrity, originality, and the diminishing importance of foundational knowledge in the legal field.

The application of AI-generated content within the context of academia upsets the conventional understanding of authorship and merit. If not carefully considered and protected against, AI-generated technology has the potential of perpetuating rote learning and reliance on AI-generated content rather than the development of sound legal reasoning skills.⁴⁹ Indeed, within the context of legal education, the development of sound critical reasoning skills and judicial responsibility is pivotal within professional training. This is particularly so from the point of view that future lawyers will inevitably interact with AI-generated technology within the legal process.

Thus, there is a need to rebalance the ways of teaching law and give more emphasis to critical thinking, ethical reasoning and interdisciplinary knowledge. The law school should educate the students, not only to use AI technology but also to question their own assumptions, boundaries, and implications within the social context. An interdisciplinary approach that puts together

⁴⁶ Danielle Keats Citron, *Technological Due Process*, 85 Wash. U. L. Rev. 1249, 1315–18 (2008).

⁴⁷ *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 (India).

⁴⁸ Richard Susskind, *Tomorrow's Lawyers: An Introduction to Your Future* 28–31 (Oxford Univ. Press 2017).

⁴⁹ John Danaher, *Automation and Utopia: Human Flourishing in a World Without Work* 87–89 (Harvard Univ. Press 2019).

learnings from technology studies, philosophy, economics, and social sciences can enable such learning.⁵⁰

Incorporation of the ethics of artificial intelligence training in law education is, then, crucial in producing a pool of legal practitioners who would be able to regulate AI appropriately in accordance with constitutional principles. Legal education is also relevant in defining a normative discourse on justice and technology, which is crucial in ensuring a future generation of legal professionals is equipped to ensure artificial intelligence does not compromise, but rather strengthens, the legal profession.⁵¹ Taking a transformation approach in ensuring artificial intelligence is beneficial to society will be critical in ensuring that artificial intelligence does not compromise, but rather strengthens, society.

10. GLOBAL GOVERNANCE AND INTERNATIONAL LAW.

AI governance operates on a global platform, making it inadequate and ineffective if handled and regulated on a local or national level. This is because AI operates and develops on a cross-border platform, while its effects, such as data mining and discrimination through algorithms, also work on a cross-border platform.⁵² If this is allowed or permitted on a national level without a common international standard, then regulatory arbitrage could become a reality since companies can decide on AI development or deployment on a platform with less strict rules and management.⁵³

International law has been very important in providing a basis for the formulation of general principles for good governance in the use of AI. The normative framework is already established in international human rights instruments on such issues as privacy, discrimination, freedom of expression and finding remedies. These principles have been very important because they have been impacted by the use of AI.⁵⁴ International law has been state-centred. However, this has been changing because there are actors whose technological capabilities are very much like those of states.⁵⁵

⁵⁰ Paul Maharg, *Transforming Legal Education: Learning and Teaching the Law in the Early Twenty-First Century*, 38 J. L. & Soc'y 1, 6–9 (2011).

⁵¹ UNESCO, *Recommendation on the Ethics of Artificial Intelligence* 44–49 (2021).

⁵² Kal Raustiala, *Governing the Internet*, 110 Am. J. Int'l L. 491, 494–96 (2016).

⁵³ Anu Bradford, *The Brussels Effect: How the European Union Rules the World* 97–100 (Oxford Univ. Press 2020).

⁵⁴ Universal Declaration of Human Rights arts. 2, 12, 19, G.A. Res. 217 (III), U.N. Doc. A/810 (Dec. 10, 1948).

⁵⁵ Philip Alston, *The Populist Challenge to Human Rights*, 9 J. Hum. Rts. Prac. 1, 7–9 (2017).

The global governance bodies must therefore take a proactive role in harmonising regulatory standards in relation to cross-boundary harm caused by AI. The multilateral bodies and regulatory groups have the best chance of crafting soft laws on issues of AI that can shape domestic laws and business practices.⁵⁶ Even though soft laws are not formally binding instruments of international law, they play a part in the convergence of norms and may be a precursor to hard laws in the future.

Thus, AI rule-setting also constitutes a major challenge for the adaptability of international law in a rapidly changing environment characterised by technological developments. Conventional rules on jurisdiction, sovereignty, and attribution between states are challenged by new and independent technologies such as AI.⁵⁷ However, for international law to remain relevant, it is also necessary for international law to move towards new rule-setting approaches that are flexible and anticipatory and that can address new risks associated with new technological developments, including AI. Through this, international law can also take a major role in developing a global AI regime that is resilient and legitimate.⁵⁸

11. CONCLUSION

Artificial Intelligence is not just a technology transformation; it is a shifting power structure that makes even the principles of the law, the regime and responsibility questionable. As algorithms are set to shape an increasing number of decisions concerning the liberties, the equality, the markets, and the access to the essential services, law cannot but change the way it regards artificial intelligence: from a neutral tool, from a technical change, to a socio-legal phenomenon that has the power to redistribute, to transform, and to redefine.

The new legal methodology must be holistic to meet the challenges that are posed by artificial intelligence as well as its threats. Ethical reasoning, justice in society, economic regulation, and international governance should work in convergence and not in seclusion. The subject-based or piecemeal approaches are not sufficient and lack the capacity to deal with the cross-cutting aspect of AI, particularly on matters that require cross-border algorithmic decision-making.

In this paper, the role that holding algorithms accountable must take on if it is to be effective and lasting is that of being rooted within the realms of the constitution and the ideals that relate

⁵⁶ Organisation for Economic Co-operation and Development (OECD), *OECD Principles on Artificial Intelligence* (2019).

⁵⁷ U.N. Secretary-General, *Roadmap for Digital Cooperation* 82–87 (2020).

⁵⁸ UNESCO, *Recommendation on the Ethics of Artificial Intelligence* 62–70 (2021).

to the promotion of human dignity and democratic ideals. It is thus the responsibility of the law to make transparency, explainability, and contestability factors of AI regulation a prerequisite.

Only a future-oriented perspective of law regulation, whereby law is regarded as an integrative, dynamic, and adaptive process, will allow proactively responding to changes introduced by technology, as opposed to merely responding to harm. By incorporating normative values into the development, use, and regulation of artificial intelligence, it will be possible to steer innovation in a socially beneficial direction. In this way, a future-oriented approach to legal regulation has the possibility of using artificial intelligence in a way that will help to move society toward a more just, equitable, and humane society.