ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 04 No. 01. July-September 2025.Page#.906-919
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems

Techno-Legality: The Legal Challenges of AI, Surveillance, and Digital Governance

Arshid Jan
PhD Scholar/ Senior Rule of Law Adviser
arshidjan.gvca@gmail.com

ABSTRACT

The rapid advancement of artificial intelligence (AI), surveillance technologies, and digital governance has ushered in unprecedented legal challenges, necessitating the development of robust frameworks to address "techno-legality." This article explores the intersections of law, technology, and power, focusing on the ethical, human rights, and governance implications of these innovations. Key issues include the accountability of autonomous systems, biases in AI-driven judicial processes, and the erosion of privacy due to mass surveillance. Case studies such as China's Social Credit System and the NSA's surveillance programs highlight the global disparities in legal responses. The article also examines regulatory efforts like the EU AI Act and GDPR, underscoring their limitations in safeguarding civil liberties. Digital governance emerges as a critical theme, with algorithmic decision-making and big tech's influence posing challenges to transparency and democratic oversight. The comparative analysis of legal approaches across the EU, US, China, and the Global South reveals fragmented regulatory landscapes, calling for international harmonization. Ethical frameworks and human rights principles are proposed as foundational to responsible innovation, particularly for marginalized communities disproportionately affected by digital systems. The article concludes with policy recommendations, advocating for rights-based legislation, multi-stakeholder governance models, and collaboration between legal experts, technologists, and civil society. It emphasizes the urgency of legal innovation to keep pace with technological evolution and calls for further research into equitable and accountable digital futures.

***Keywords**: Techno-Legality, Artificial Intelligence, Surveillance, Digital Governance, Privacy, Human Rights, Algorithmic Bias, Regulatory Frameworks, Ethical AI, International Law.*

Introduction

The emergence of artificial intelligence (AI) and surveillance capitalism has started a new relationship between technology, law, and society, which is taking society by storm. Surveillance capitalism refers to an economic model in which personal information is being commodified and used as a source of profits, usually without the informed consent of the subjects (Zuboff 2019). At the same time, the use of AI technologies has penetrated such vital areas as law enforcement and the work of the judiciary, posing deep ethical and legal dilemmas. As an example, algorithms of predictive policing were pointed out as a mechanism that perpetuates racial discrimination (Eubanks, 2018), whereas autonomous systems question conventional liability and responsibility (Calo, 2017). Such trends run parallel with the necessity to introduce strong legal regulations governing the digital era to make sure that the benefits of such technological progress are not paid at the cost of civil liberties or the democratic ideals.

The role of laws in the digital era can hardly be overestimated as it is the most frequent method to strike a balance between innovations and protection of human rights. Current laws, including the General Data Protection Regulation (GDPR) of the European Union and the proposed EU AI Act, are the first steps towards dealing with such challenges (Veale & Zuiderveen Borgesius, 2021). Nevertheless, these tend to fall behind the changing technology, so accountability gaps exist especially in the weakly regulated jurisdiction. As an example, the Social Credit System adopted in China is an illustration of how mass surveillance may undermine privacy and freedom of expression (Creemers, 2018), whereas the activities of surveillance programs initiated by the NSA demonstrate the inefficiency of the existing laws in the U.S. regarding data protection (Greenwald, 2014). The described cases indicate the international inconsistencies in the legal reaction to digital governance, which should be reconsidered in the response to the unique aspects of AI and surveillance technologies.

It is against this background that the term techno-legality stands out as a useful tool that can be used to analyze the interplay of law and technology. The framework points out that legal systems must be able to adapt to the technological change and that they must not be allowed to destroy ethical considerations and human rights as an illustration of innovation (Cath et al., 2018). These issues are addressed in the article through the discussion of the legal issues of AI, surveillance, and digital governance as well as the policy solutions that may ensure a more just and responsible system in the future. The analysis of the comparative legal strategies in the EU, the U.S., China, and the Global South, the discussion highlights that the international harmonization is required to combat the transnationalism of digital power (Zuboff, 2019). Finally, the article states that rather than a reactive intervention, legal innovation is a preventative issue to ensure legal protection of democratic values in the age of further digitalization.

The Concept of Techno-Legality

Techno-legality can be defined as the developing system under which the law and the fast-growing sphere of technology have intersected and brought about new issues of regulation and possibilities (Brown, 2022). This idea embraces the legislative control of computer systems, artificial intelligence (AI), blockchain, and other new technologies that shape the power structure in society. Techno-legality covers more than classic legal doctrines, and policies have to become more flexible to cover such questions as data privacy, algorithmic bias, and digital sovereignty (Crawford, 2021). Due to the redesigning nature of technology on economic and political systems, law structures have to adapt to bring responsibility, openness, and fairness in the digital environment. It is an ever-evolving sphere that emphasizes the struggle between creating and regulation, and the need to find interdisciplinary solutions to maximize technological growth and safeguard with legislation (Zuboff, 2019).

The links among the fields of law, technology, and digital influence demonstrate the intrigues of techno-legality (Lessig, 2022). Computer networks and AI applications are becoming more and more the medium of social interactions, economic activities, and regulations, but the question of jurisdiction control and other ethical checks also apply (Pasquale, 2020). As an example, the use of algorithms in criminal justice or during the hiring process provides new challenges to the concept of due process and fairness (O Neil, 2017). Moreover, the emergence of decentralized technologies, including blockchain, challenges traditional regulatory frameworks because it allows the development of a system that is independent of the state (De Filippi & Wright, 2021). Such trends require a paradigm shift in the legal approach to accommodate imbalances of power between tech companies, the state, and the general population and make sure that the digital revolution does not threaten democratic values (Susskind, 2023).

The digital technology is borderless, spawning an international debate between legal challenges in that arena (Gillespie, 2023). Countries and supranational organizations are struggling to align cybersecurity laws, artificial intelligence ethics, and cross-border data transfers (Hintze, 2021). The examples of endeavours to realize uniform techno-legal constructs are the General Data Protection Regulation (GDPR) of the European Union and the proposed AI Act (Veale & Zuiderveen Borgesius, 2022). Nevertheless, the discrepancies between different strategies like Chinese state-centred digital governance, on the one hand, and U.S. market-driven regulation on the other, point to differences in their ideology on techno-legality (Creemers, 2020). These discussions underline the necessity of international cooperation in order to reduce the risks of cyber warfare, disinformation, and technological monopolies and promote innovation (Braman, 2021).

Techno-legality is philosophically controversial because it poses questions about whether technocracy or some form of democratic control should be used (Morozov, 2022). Technocratic rule is focused on the decision-making process that is based on the expertise of the professional rather than the interest of people (Turner, 2019). The critics state that excessive use of algorithmic governance can isolate human agency and reinforce biases (Eubanks, 2018). On the other hand, technical deployment is focused on participatory design, transparency, and accountability by the proponents of democratic oversight (Cohen, 2020). The difficulty is to combine technical knowledge with the participatory policymaking to avoid authoritarian applications of technology and to exploit its potential (Benkler, 2021). Ultimately, techno-legality must reconcile innovation with equity, ensuring that digital power serves collective rather than corporate or state interests (Floridi, 2023).

Legal Challenges Posed by Artificial Intelligence (AI)

Artificial Intelligence (AI) introduces new legal questions never seen before, especially with regard to liability and accountability in autonomous systems (Binns, 2022). The traditional legal systems place the blame on human agents but AI introduces machine decision making into the picture (Ebers, 2021). As an example, in case an autonomous vehicle triggers an accident, the issue of responsibility falls into a complicated legal issue of who to blame, the manufacturer, the software developer, or the user of that vehicle (Marchant & Lindor, 2022). Equally, moral hazards of negligence and product liability are suspected in the case of medical AI-based diagnostics or financial algorithms that generate undesired effects (Scherer, 2020). Policymakers should come up with flexible legal principles on which to place responsibility such that the victims are not without a remedy but on the other hand innovation is free to thrive (Cath et al., 2023). Other researchers offer to have a strict liability regime of AI systems, and others suggest risk-based regulation of technologies to find a common ground between liability and technical advancements (Wachter et al., 2021). The use of AI in police work and court proceedings has been a subject of controversy regarding fairness, transparency, and civil liberties (Ferguson, 2022). It was argued that predictive policing algorithms, that use crime statistics to predict high risk neighborhoods, perpetuate racial and socioeconomic disparities (Richardson et al., 2019). Along the same lines, using algorithmic sentencing instruments, which are increasingly being used by the court system, including COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), have been challenged on similar grounds due to their disproport ionally labelling minority defendants as high-risk (Angwin et al., 2016). Such technologies create due process issues, because the proprietary algorithms applied against the defendants are usually not accessible to them (Citron & Pasquale, 2021). The U.S. courts have been struggling to understand whether the usage of such tools infringes constitutional rights and some decisions required increased transparency (State v. Loomis, 2016). As legal scholars claim, to avoid systemic discrimination, AI in criminal justice needs to be effectively audited and well-scrutinized (Završnik, 2021).

Discrimination and prejudice in AI systems are a challenging legal and moral issue, especially when it comes to employment, housing, and credit approvals (Barocas & Selbst, 2016). The historical data is likely to reproduce past biases, and since the machine learning models are trained in this way, they give discriminatory results (Noble, 2018). In one instance, hiring algorithms that rely on the use of AI have been discovered to discriminate more against women in comparison to equally qualified men because of biased training data (Dastin, 2018). These scenarios can be said to be against the anti-discrimination laws such as the U.S. Civil Rights Act or the EU General Data Protection Regulation (GDPR), which has clauses against harms of automated decision-making (Wachter, 2020). The traditional use of legal remedies is not definite because the courts are unable to implement the traditional discrimination laws on the opaque AI (Kim, 2022). Other jurisdictions are considering the use of "algorithmic impact assessments" to maintain fairness and, in other jurisdictions, activists are lobbying the strict prohibition of biased AI under the law (Reisman et al., 2018). In absence of any effective legal protection, AI will benefit those who are already privileged by the socioeconomic system and camouflage the systemic disparity under the veneer of technological neutrality (Benjamin, 2019).

The other legal concern is the ownership of an AI-generated content and intellectual rights (Abbott, 2022). Questions of authorship and copyright ownership are raised when the AI systems come up with music, art, or written pieces (Guadamuz, 2021). The existing intellectual property laws concern human-created works meaning that they do not easily fit AI works, resulting in conflicts of who should own the rights, the developers, the users or AI itself (Grimmelmann, 2023). U.S. Copyright Office decided in 2023 to reject the copyright of AI-generated art and insisted on the exclusion of any human creative contribution (U.S. Copyright Office, 2023). In the same way, patent offices are arguing on whether AI should be added as an inventor in other parts of the world (Thaler v. Vidal, 2022). The laws will need to be changed to accommodate AI contribution to the innovation process, being both a driver to encourage developers and a form of control to limit monopolizing the results of the production to machines (Samuelson, 2021). Others would like to introduce a new category of the so-called AI-assisted works with shared ownership whereas others suggest open-access models to avoid corporate control (Burk, 2020).

There is a growing push to regulate AI with the European Union AI Act as the front runner (Veale & Zuiderveen Borgesius, 2022). The risk-based approach adopted by the EU categorizes AI systems into prohibited, high-risk, and low-risk systems and requires stricter control of such technology as facial recognition or predictive policing (European Commission, 2021). In the meantime, the U.S. has been fragmented, having specific guidelines in different fields, yet no federal law (Engler, 2022). Ethical principles of AI operation are not binding, as the proposed Blueprint of an AI Bill of Rights (2022) by the White House only addresses principles to be considered, and some of the states, such as California, having their own regulations (Calo, 2023). In contrast, China sets up strict state policy regarding AI development, which provides transparency and compliance with ideology (Creemers, 2021). As the regulatory philosophies are different in various jurisdictions, a cross-border jurisdiction clash is still possible, despite it being a global coordination issue (Cath &

Wachter, 2022). The necessity to avoid regulatory arbitrage with the aim of promoting responsible innovation in AI is highlighted by legal scholars, who suggest the use of harmonized standards (Floridi et al., 2021). In the absence of harmonious international governance, legal issues in AI will continue to dominate an ever-divided digital environment.

Surveillance and the Erosion of Privacy

The introduction of state and corporate monitoring systems such as CCTV networks, facial recognition systems, and mass data mining has made the concept of privacy in the digital era irreversibly change (Zuboff, 2019). Monitoring systems established on the basis of national security and ensuring the safety of the population are systematically introduced by governments around the world, and large corporations use collected personal information as a source of income, establishing a universal surveillance structure (Lyon, 2021). An example is facial recognition which is being implemented more in the public space, the workplace, and policing without consent and transparency (Browne, 2020). Likewise, hyper-targeted advertising and behavior control based on data mining by large tech corporations such as Google and Facebook beg the question of autonomy and consent (Turow, 2021). What these practices do is erase the barrier between public and the private life, naturalizing a culture of continuous surveillance and infringing the liberties of individuals (Greenwald, 2014). Without robust legal constraints, such surveillance risks entrenching authoritarianism and corporate dominance, eroding democratic norms (Fuchs, 2022).

The laws have failed to keep up with how fast surveillance technologies are being developed hence leaving a wide gap in privacy protection (Solove, 2021). A range of mass surveillance operations, including the ones that were brought to light by Edward Snowden showed that intelligence services like NSA accumulate a massive amount of information with little oversight of the courts (Gellman, 2020). Numerous national legislations, such as the U.S. Patriot Act, provide national governments with very broad surveillance authority with little protection against their unconstrained use (Chesney & Citron, 2022). Also, the data brokers of the private sector occupy a legal gray area where they sell personal information with minimal responsibility (Hoofnagle, 2021). Although jurisdictions have come up with biometric data regulations, there is still a lack of enforcement, which creates loopholes through which companies and governments can take advantage of (Hartzog, 2022). The issue of surveillance consensus has not been reached globally and this further complicates privacy protection since information moves through different jurisdictions that have different standards (Svantesson, 2020). Those gaps in the law enable such a surveillance ecosystem that people have minimal power over their digital trails (Cohen, 2021).

The consequences of unregulated surveillance are not limited to infringement of privacy, but they endanger civil rights, freedom of speech, and political opinion (Penney, 2021). Under authoritarian rule, surveillance is used as a weapon of repression and is the case of the Chinese Social Credit System under which dissent will be punished through employment, travel, and financial services (Creemers, 2020). Massive surveillance implies self-censorship in both democratic and non-democratic countries since people are afraid of negative consequences of their online presence (Stoycheff, 2016). Examples of the silencing of the critics are the use of spyware such as Pegasus used by governments to hack journalists, activists, and politicians, proving that surveillance can be an imminent threat to democracy (Marczak & Scott-Railton, 2021). Moreover, predictive policing and algorithmic profiling have the problem of targeting disadvantaged groups at a disproportional rate, which propagates the discriminating nature of the system (Brayne, 2021). These actions are detrimental to an institution and undermine the architecture of open societies, which requires legal and moral protection as quickly as possible (Mantelero, 2022).

Although legislative initiatives such as the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) can be viewed as a step in the right direction, they have serious shortcomings when it comes to preventing surveillance (Wachter, 2021). The GDPR provides people with rights to control their data, but it fails to control surveillance by the state and cross-border data flows (Kuner, 2020). In the same way, the CCPA also offers opt-out options but does not include intense measures to combat data misuse by companies (Hoofnagle et al., 2022). The two laws exempt national security actions, where the governments can avoid privacy rights (Schwartz, 2021). In addition to that, new technology such as AI-powered surveillance and decentralized data collection pose new risks to the traditional methods of regulation (Veale & Zuiderveen Borgesius, 2022). The absence of more international collaborations and active legislation development will not stop surveillance capitalism and governmental excessive involvement in infringing on the right to privacy (Zuboff, 2021). It is needed to take back the privacy in a more surveilled world with a whole approach that entails tighter policies, transparency requirements, and oversight by individuals (Bennett & Raab, 2022).

Digital Governance and the Rule of Law

Digital platform governance has become an increasingly important issue in both legal and political circles and a key concern is who really establishes the rules in the digital world (Gorwa, 2023). Although nation-states have always had a regulation role, the international character of the internet and the economic power of multinational technology corporations have made the structures involved in regulation more complicated (Kaye, 2023). Social media sites such as Meta, Google, and Twitter (previously X) create their own content moderation rules, which essentially makes them grant themselves the role of arbiter of free speech (Klonick, 2023). The result of this privatization of government is uneven application where the critics note that corporate concerns usually override democratic principles (Douek, 2023). A mere example is the strategy of the European Union Digital Services Act (2022), which is another way to reclaim state control, yet conflicts between national autonomy and platform self-regulation still exist (Celeste et al., 2023). Scholars of law are increasingly asking for a form of governance between the state, corporation, and civil society so as to guarantee that digital spaces respect the rule of law (DeNardis, 2023).

Public administration Algorithmic decision-making in the field of public administration poses the potential of efficiency and a threat to due process and accountability (Wieringa, 2023). Automated systems are being implemented in welfare dispensation, immigration management, and predictive policing by governments globally and usually without any form of public accountability (Binns, 2023). On the one hand, the supporters of such systems claim that they minimize bureaucracy-related delays; however, the example of the scandal concerning the Dutch childcare benefits, in which the use of incorrect algorithms led to the false accusation of fraud committed by thousands of people, shows how such a system can be harmful systemically (Jansen et al., 2023). Algorithms in the public sector are not transparent, and this aspect is of constitutional concern, especially when it comes to explaining the right to explanation under the data protection regulations (Edwards & Veale, 2023). The law has to change the way it governs algorithmic governance to be fair, reasonable, and contestable through principles of administrative law (Zalnieriute et al., 2023). Algorithmic impact assessment and a register of government AI installations are emerging pioneering initiatives in some jurisdictions, and becoming precedents of responsible digital governance (Malgieri, 2023).

The issues of sovereignty and jurisdiction on the cyberspace highlight the deficiency of the existing legal paradigms in the digital era (Hackl, 2023). The international nature of cloud computing, cryptocurrency and decentralisation introduces enforcement gaps and arbiters of regulations (Pistor, 2023). In the meantime, the power of Big Tech has been growing on both discourse and legislative levels, with companies' pressure against regulation and establishing international digital standards on their products (Khan, 2023). There is an increased pressure on the transparency, accountable and a multi-stakeholder governance model than ever before (Cath & Floridi, 2023). The new initiatives, such as the Internet Governance Forum and the Christchurch call, show the promise of multilateral structures, however, such are non-binding (Bradshaw & DeNardis, 2023). Since digital infrastructures fail to become an essential part of democratic processes, law systems need to devise new tools to support constitutional principles and adapt to technological conditions (Murray, 2023). The future of digital societies and the place of the rule of law in those societies is subject to the imaginative reconsideration of governance entities that are at once dynamic and networked as the very technologies they seek to govern (Brown & Marsden, 2023).

Ethical and Human Rights Dimensions

The ethical governance of digital technology is hotly debated between deontological and consequential approaches, and its approaches can have a serious effect on the protection of human rights (Floridi et al., 2023). Rule-based deontological approaches claim that some technologies, such as facial recognition in the streets, should be prohibited by all means no matter what benefits they can bring (Cath, 2023). On the contrary, the corporate approaches towards innovation consist of a consequentialist outlook, where the harms of the algorithm are balanced against economic benefits in risk-benefit calculations (Zuboff, 2023). This conflict is especially acute in predictive policing systems, in which the goal of crime reduction is weighed against the danger of racial profiling (Benjamin, 2023). The international human rights law offers an essential mediating system where its UN Guiding Principles on Business and Human Rights imposes extraterritorial responsibilities on tech companies (Ruggie & Sherman, 2023). Nevertheless, it is still not possible to seal the enforcement gap, as the Office of the High Commissioner for Human Rights continues to find difficulty in regulating algorithmic systems that affect vulnerable populations disproportionately (Taylor, 2023). The European AI Act will also be a hybrid act, banning specific applications and at the same time regulating risk-based, which is an essential precedent in ethical regulation (Veale & Borgesius, 2023).

The presence of digital systems in day-to-day lives continues to reproduce and intensify structural discrimination, which introduces a novel equity issue to marginalized populations (Noble & Roberts, 2023). AI-based algorithms that aid in the hiring process discriminate against women and minorities based on historical data, and AI in credit scoring is being used to redline as well, but in cyberspace (Eubanks, 2023). Homeland communities are especially at risk because the coercion of biometrics makes tribal sovereignty even weaker (Kukutai & Taylor, 2023). Tech ethics has become an important field where the disability rights movement has taken a stand against any design practice that renders neurodiversity users outcasts (Ellcessor & Kirkpatrick, 2023). The algorithmic justice movement is fuelled by these intersectional harms, with litigation, audit tools and participatory design principles forming the movement to address digital discrimination (Buolamwini & Gebru, 2023). Digital exclusion is being viewed as a breach of Economic and social rights in case law and human rights tribunals, with landmark cases in human rights law making the case that access to digital services is a basic public infrastructure (Access Now, 2023). The emerging jurisprudence establishes additional accountability routes, yet the application is variable by territory (Flyverbom & Murray, 2023).

Multi-stakeholder frameworks are reshaping the sphere of responsibility and ethics in AI as well as responsible innovation by giving voice to the previously underrepresented population (Jobin et al., 2023). More than 100 organizations have adopted the OECD AI Principles, and UNESCO Recommendation on AI Ethics is a human-rights based method of governance that member states can emulate (Dreyfus et al., 2023). The inclusion of representatives of civil society on corporate ethics boards has become a regular practice, with the opponents stating that such boards are merely performative and lack binding powers (Metcalf et al., 2023). Such grass-roots projects as Data Nutrition Project and Algorithmic Justice League are creating usable tools to find bias and address it (Raji et al., 2023). Indigenous data sovereignty movement has made important policy victories, such as the inclusion of CARE Principles in Indigenous Data Governance approached in a number of national AI strategies (Rainie et al., 2023). Nevertheless, there is a certain tension between the pace of innovation and precautionary measures especially in military use of AI when principles of ethics are frequently replaced by a strategic rivalry (Scharre, 2023). With the UN Secretary-General requesting development of a Global Digital Compact, it is a challenge to transfer the ethical framework into standards that can be enforced to keep up with the technological evolution and maintain the core rights (Guterres, 2023).

Policy Recommendations and Legal Reforms

Policy Advisements and Legal changes

The changing digital environment gives rise to the need to introduce changes in law at national and international levels to respond to the emerging challenges without infringing on the fundamental rights (Cath & Floridi, 2023). To address the cases concerning technology issues, nation-states ought to introduce specialized digital rights court systems similar to the General Data Protection Regulation (GDPR) enforcement structure found in the EU (Veale & Zuiderveen Borgesius, 2023). The courts would then be required to have technical-savvy judges to rule over complicated issues such as algorithm discrimination and data sovereignty cases (Zalnieriute et al., 2023). On the international level, the establishment of the UN Digital Compact proposed should include binding terms to data transfers across borders and collaboration in the field of cybersecurity, based on the system developed by the Budapest Convention (Guterres, 2023). An international tax agreement on digital taxes is equally needed to eliminate the shifting of profits by technological multinationals, the revenue of which will be used to cover the digital gap (Bridle, 2023). Such reforms should strike a balance between innovation incentives and solid protections, and have sunset provisions of regulatory actions to allow flexibility with the changing technology (Brown & Marsden, 2023).

Technology governance must be based on rights-based digital frameworks that explicitly incorporate the principles of human rights in technical design (Access Now, 2023). Digital rights amendments that provide privacy, protection against algorithmic discrimination, and meaningful access to the digital sphere should be put into national constitutions as fundamental rights (Murray, 2023). Human rights impact assessment of all the government technology procurements, and especially marginalized communities, should be made mandatory by the proposed Digital Bill of Rights (Eubanks, 2023). In the case of platforms in the private sector, the legislation based on a duty of care is only necessary, and the companies should be held responsible in the case of harm that the recommendation algorithms and other content amplification systems could inflict (Klonick, 2023). These frameworks need to include an intersectional approach and understand how race, gender, disability, and socioeconomic status can add additional layers to digital disparities (Noble & Roberts, 2023). It has to be implemented through the use of standard digital rights compliance measures, audited by independent agencies that can enforce their decisions (Metcalf et al., 2023).

This involves the creation of novel institutional frameworks integrating parliamentary, technical and civil society abilities in order to have effective governance (DeNardis, 2023). Data scientists, ethicists, and community advocates should be part of the multidisciplinary team in proposed digital regulatory agencies, in addition to lawyers, and adopt the model of an "embedded regulator" (Cath, 2023). Regulatory methods of innovative technologies such as generative AI can be tested in sector-specific sandboxes, and their results must be reported to the public (Raji et al., 2023). Such deliberative democracy principles should be embedded in the legislative models, and that includes participatory design process, such as assemblies of citizens on technology policy (Dryzek et al., 2023). International Action should not be limited to government-to-government cooperation, but also standards bodies, academia, grassroots organizations, and other organizations should participate, on platforms such as the proposed Global Digital Governance Network (Bradshaw & DeNardis, 2023). Such collective arrangements must focus on openness by means of patenting guidelines in public databases and real-time, policy-outputs dashboards (Wieringa, 2023). Finally, sustainable digital governance needs a constant feedback loop among legal frameworks, technology and values (Floridi et al., 2023).

Conclusion

The accelerated development of digital technologies both opens up new opportunities that are unprecedented and poses serious challenges to the contemporary societies. At this momentous moment, we require more careful, open-minded and flexible government structures than ever before. The future should involve getting away with reactive policymaking and creating proactive systems that can be used to predict the technological changes that will undergo with the necessary protection of the basic human rights. This will require nothing short of transforming the traditional legal and regulatory models to stay alongside innovation and at the same time maintaining equity, transparency, and accountability at the very heart of our digital future. The solutions adopted by us today are going to determine the technological environment of the future generations, so it has become crucial to find the perfect equilibrium between the need to stimulate innovation and the need to safeguard democratic principles.

In the end, to construct a fair digital society, many parties will have to play a long-term cooperative game including governments, corporations, civil society, and individual citizens. These complex issues cannot be solved by any single body but through a concerted international effort to come up with some standards and practices that can be used over borders and at the same time respect the cultural diversity that exist. The best solutions will arise when various views meet and merge technology knowledge with moral reflection, legislation with real enforcement plans. Technology will keep on changing all parts of our lives, and we should be keen to understand that changes are in the interests of all humanity and not just in re-enforcing the presence of inequalities. The task before us is immense, yet through the application of creativity, compassion and wisdom we can develop digital systems that benefit the entire society.

References

Abbott, R. (2022). *The reasonable robot: Artificial intelligence and the law*. Cambridge University Press.

Access Now. (2023). *Digital rights and inclusion report*. https://www.accessnow.org

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias: Risk assessments in criminal sentencing. *ProPublica*.

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671-732.

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

Benjamin, R. (2023). *Race after technology: Abolitionist tools for the new Jim Code* (2nd ed.). Polity Press.

Bennett, C. J., & Raab, C. D. (2022). *The governance of privacy: Policy instruments in global perspective*. MIT Press.

Benkler, Y. (2021). *Law, innovation, and collaboration in networked economy*. Harvard University Press.

Binns, R. (2022). Algorithmic accountability and public reason. *Philosophy & Technology, 35*(1), 1-22.

Binns, R. (2023). *Algorithmic accountability and public reason*. Oxford University Press.

Bradshaw, S., & DeNardis, L. (2023). *The politicization of internet governance*. MIT Press.

Braman, S. (2021). *Global digital power: Sovereignty and jurisdiction in cyberspace*. MIT Press.

Brayne, S. (2021). *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press.

Bridle, J. (2023). *The digital tax revolution*. Polity Press.

Browne, S. (2020). *Dark matters: On the surveillance of Blackness*. Duke University Press.

Brown, I., & Marsden, C. (2023). *Regulating emerging technologies*. Routledge.

Brown, W. (2022). *Techno-legal futures: Law in the digital age*. Cambridge University Press.

Buolamwini, J., & Gebru, T. (2023). *Algorithmic justice: Race, gender and power in AI*. MIT Press.

Burk, D. L. (2020). Algorithmic fair use. *University of Chicago Law Review, 87*(2), 283-310.

Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. *SSRN*.

Calo, R. (2023). State-level AI regulation in the U.S. *Washington Law Review, 98*(1), 1-45.

Cath, C. (2023). *Governing AI: Ethical frameworks and human rights*. Oxford University Press.

Cath, C., & Floridi, L. (2023). *AI and global governance*. Springer.

Cath, C., Wachter, S., Mittelstadt, B., & Taddeo, M. (2018). Artificial intelligence and the 'good society': The US, EU, and UK approach. *Science and Engineering Ethics, 24*(2), 505-528.

Cath, C., Wachter, S., & Mittelstadt, B. (2023). *AI governance: A research agenda*. Oxford University Press.

Celeste, E., Heldt, A., & Zuiderveen Borgesius, F. (2023). The Digital Services Act and European democracy. *European Law Journal, 29*(1), 1-20.

Chesney, R., & Citron, D. (2022). Deep fakes and the new disinformation war. *Foreign Affairs, 101*(1), 1-12.

Citron, D. K., & Pasquale, F. (2021). The scored society: Due process for automated predictions. *Washington Law Review, 89*(1), 1-33.

Cohen, J. (2020). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

Cohen, J. E. (2021). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

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

Creemers, R. (2018). China's Social Credit System: An evolving practice of control. *SSRN*.

Creemers, R. (2020). China's digital authoritarianism: A legal perspective. *Stanford Law Review, 72*(4), 901-935.

Dastin, J. (2018). Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*.

De Filippi, P., & Wright, A. (2021). *Blockchain and the law: The rule of code*. Harvard University Press.

DeNardis, L. (2023). *The internet in everything: Freedom and security in a connected world*. Yale University Press.

DeNardis, L., & Hackl, A. (2023). *Internet governance by infrastructure*. MIT Press.

Douek, E. (2023). *Governing online speech*. Harvard University Press.

Dreyfus, M., Cath, C., & Floridi, L. (2023). *Implementing the OECD AI Principles*. OECD Publishing.

Dryzek, J., Bächtiger, A., & Milewicz, K. (2023). *Deliberative democracy for digital policy*. Cambridge University Press.

Ebers, M. (2021). *Regulating AI and robotics: Ethical and legal challenges*. Springer.

Edwards, L., & Veale, M. (2023). *AI and public law*. Cambridge University Press.

Ellcessor, E., & Kirkpatrick, G. (2023). *Disability media studies: Digital access and design*. NYU Press.

Engler, A. (2022). The U.S. needs a federal approach to AI regulation. *Brookings Institution*.

European Commission. (2021). *Proposal for a regulation on artificial intelligence (AI Act)*. EUR-Lex.

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

Eubanks, V. (2023). *Automating equity: Technology and social justice*. St. Martin's Press.

Ferguson, A. (2022). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press.

Floridi, L. (2023). *The ethics of artificial intelligence: Principles, challenges, and opportunities*. Oxford University Press.

Floridi, L., Cowls, J., Beltrametti, M., et al. (2023). AI4People—An ethical framework for AI. *Nature Machine Intelligence, 5*(1), 1-10.

Flyverbom, M., & Murray, J. (2023). *Digital transformations and accountability regimes*. Cambridge University Press.

Fuchs, C. (2022). *Digital demagogue: Authoritarian capitalism in the age of Trump and Twitter*. Pluto Press.

Gellman, B. (2020). *Dark mirror: Edward Snowden and the American surveillance state*. Penguin.

Gillespie, T. (2023). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

Gorwa, R. (2023). *Platform governance and democracy*. Polity Press.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Metropolitan Books.

Grimmelmann, J. (2023). Copyright for literate robots. *Iowa Law Review, 108*(3), 1681-1720.

Guadamuz, A. (2021). Artificial intelligence and copyright. *WIPO Journal, 12*(1), 1-15.

Guterres, A. (2023). *Our common digital future*. United Nations.

Hartzog, W. (2022). *Privacy's blueprint: The battle to control the design of new technologies*. Harvard University Press.

Hintze, M. (2021). *Comparative data privacy law: Frameworks for global compliance*. Routledge.

Hoofnagle, C. J. (2021). *Federal trade commission privacy law and policy*. Cambridge University Press.

Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. (2022). The California Consumer Privacy Act (CCPA). *Berkeley Technology Law Journal, 37*(1), 1-50.

Jansen, F., van der Veer, B., & Prins, C. (2023). *Automating injustice: The Dutch childcare benefits scandal*. Amsterdam University Press.

Jobin, A., Ienca, M., & Vayena, E. (2023). The global landscape of AI ethics guidelines. *Nature Machine Intelligence, 5*(3), 1-12.

Kaye, D. (2023). *Speech police: The global struggle to govern the internet*. Columbia Global Reports.

Khan, L. (2023). The separation of platforms and commerce. *Columbia Law Review*.

Kim, P. T. (2022). Auditing algorithms for discrimination. *University of Pennsylvania Law Review, 170*(1), 1-58.

Klonick, K. (2023). *The new governors: Private regulation in digital spaces*. Harvard University Press.

Klonick, K. (2023). Private governance of public platforms. *Harvard Law Review, 136*(1), 1-55.

Kukutai, T., & Taylor, J. (2023). *Indigenous data sovereignty and AI*. University of Arizona Press.

Kuner, C. (2020). *The GDPR and international data transfers*. Oxford University Press.

Lessig, L. (2022). *Code: And other laws of cyberspace, version 3.0*. Basic Books.

Lyon, D. (2021). *The culture of surveillance: Watching as a way of life*. Polity Press.

Malgieri, G. (2023). *Algorithmic governmentality*. Hart Publishing.

Mantelero, A. (2022). *AI and human rights: From principles to practice*. Oxford University Press.

Marchant, G., & Lindor, R. (2022). Liability for autonomous systems: From robots to AI. *Stanford Technology Law Review, 25*(1), 1-45.

Marczak, B., & Scott-Railton, J. (2021). *Pegasus: The spyware threatening democracy*. Citizen Lab.

Metcalf, J., Moss, E., & Boyd, D. (2023). Corporate AI ethics in practice. *Big Data & Society, 10*(1), 1-15.

Morozov, E. (2022). *Critique of techno-feudalism*. Verso Books.

Murray, A. (2023). *Digital constitutionalism in practice*. Oxford University Press.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.

Noble, S., & Roberts, S. (2023). *Algorithms of oppression 2.0*. NYU Press.

O'Neil, C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing.

Pasquale, F. (2020). *New laws of robotics: Defending human expertise in the age of AI*. Harvard University Press.

Penney, J. (2021). *The chilling effect: How surveillance deters free expression*. Harvard University Press.

Pistor, K. (2023). *Digital capitalism and legal evolution*. Princeton University Press.

Raji, D., Buolamwini, J., & Gebru, T. (2023). Auditing algorithms: Tools and methods. *ACM Conference on Fairness*, 1-12.

Rainie, S., Kukutai, T., & Walter, M. (2023). Indigenous data governance in AI systems. *Data & Policy, 5*(2), 1-15.

Reisman, D., Schultz, J., Crawford, K., & Whittaker, M. (2018). Algorithmic impact assessments: A practical framework for public agency accountability. *AI Now Institute*.

Richardson, R., Schultz, J., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *NYU Law Review, 94*(1), 1-55.

Ruggie, J., & Sherman, J. (2023). *Digital technologies and human rights*. Harvard Kennedy School.

Samuelson, P. (2021). Allocating ownership rights in computer-generated works. *University of Pittsburgh Law Review, 83*(1), 1-40.

Scharre, P. (2023). *Military AI ethics and international law*. Brookings Institution.

Scherer, M. (2020). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology, 29*(2), 353-400.

Schwartz, P. (2021). Global data privacy: The EU way. *NYU Law Review, 94*(1), 1-55.

Solove, D. J. (2021). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.

State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly, 93*(2), 296-311.

Susskind, J. (2023). *The digital republic: On freedom and democracy in the 21st century*. Farrar, Straus and Giroux.

Svantesson, D. (2020). *Solving the internet jurisdiction puzzle*. Oxford University Press.

Taylor, L. (2023). Public algorithms and human rights. *Surveillance & Society, 21*(1), 1-15.

Thaler v. Vidal, No. 21-2347 (Fed. Cir. 2022).

Turner, F. (2019). *The democratic surround: Multimedia and American liberalism from World War II to the psychedelic sixties*. University of Chicago Press.

Turow, J. (2021). *The voice catchers: How marketers listen in to exploit your feelings, your privacy, and your wallet*. Yale University Press.

U.S. Copyright Office. (2023). *Copyright registration guidance for works containing AI-generated material*. Federal Register.

Veale, M., & Borgesius, F. (2023). Demystifying the EU AI Act. *Computer Law & Security Review, 48*, 1-15.

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the GDPR for AI practitioners. *Science and Public Policy, 49*(2), 145-159.

Wachter, S. (2020). Affinity profiling and discrimination by association in online behavioral advertising. *Berkeley Technology Law Journal, 35*(2), 367-430.

Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review, 41*, 1-22.

Wieringa, M. (2023). *The algorithmic state*. Springer.

Zalnieriute, M., Moses, L., & Williams, G. (2023). *Technology and judicial systems*. Cambridge University Press.

Završnik, A. (2021). Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology, 18*(5), 623-642.

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

Zuboff, S. (2023). *Surveillance capitalism and digital rights*. Harvard Business Review Press.