IRSHAD
International Journal of Law and Policy |
Volume: 3, Issue: 9
2025

Justice and Ethical Considerations in the Digital Age

Jamil Ahmad Khokhar
Lahore Leads University

Abstract

The Research investigated justice and ethical relationships within digital Pakistan by evaluating local legislation against worldwide benchmarks along with investigating protective flaws for human rights. Digital governance in Pakistan is studied under data privacy, algorithmic fairness and surveillance and access perspectives. The research indicates that cyber laws of Pakistan establish state authority above individual liberties through PECA's ambiguous components that enable censorship and unwarranted detentions and insufficient data management leaves citizens susceptible to exploitation. Despite court orders Pakistan maintains ongoing internet shutdowns while public and private sectors use uncontrolled algorithms and lack corporate responsibility functions to limit digital rights. The article demonstrates that these system weaknesses establish a surveillance-heavy environment which chokes innovative progress and destroys trust within public society. Pakistan differs substantially from modern global digital practices that unite tech progress with protection of human rights during content moderation while handling AI ethics and digital exchange regulations.

Keywords: Digital Justice, Ethical Technology, Data Privacy Laws, Algorithmic Bias, Human Rights in Digital Age

APA Citation:

Ahmad, J. (2025). Justice and Ethical Considerations in the Digital Age. *International Journal of Law and Policy, 3* (9), 21-32. https://doi.org/10.59022/ijlp.363

I. Introduction

Digital technology transformed nearly the entire spectrum of contemporary life through its effects on communication systems and healthcare facilities as well as governmental processes and companies. The digital transformation has delivered exceptional advantages including efficiency and global access together with information accessibility (Brynjolfsson & McAfee,2014). The massive technological changes have introduced substantial moral dilemmas combined with unjust distribution of benefits and misuse of artificial intelligence technologies and unequal digital access patterns. So that it is needs to resolve present-day ethical issues of technology development because digital innovation needs to serve all members of society similarly.

In current technology-based times justice and ethics represent principles that require technology systems to operate with fair treatment alongside accountability and transparency measures. Distributive justice principles which determine fair resource distribution need implementation in digital technology to prevent worsening current social inequalities (Rawls, 1971). The ethical matters of data privacy and consent alongside autonomy require priority to shield people from data exploitation in modern information societies (Floridi, 2018). Researchers want to examine how justice and ethical concerns link up in digital times as well as identify the problems associated with this relationship. The analysis requires both responsible technologic development frameworks and research of essential matters which include algorithmic bias and AI ethics as well as digital surveillance and policymaker oversight on technology.

This article highlights the requirement to integrate moral standards into digital innovation development that leads to building a just and inclusive society. This is their primary aim of receiving this study to aid in building a comprehensive legal framework that supports responsible digital innovation while ensuring justice and ethical integrity in an era of digital prominence by examining the ethical implications of digital technologies, such as data privacy, the relevance of algorithmic bias, and AI accountability; analyzing the impact of digital systems on fairness and justice, focusing on discrimination, surveillance, and the digital divide; and investigating regulatory and policy measures for creating ethical tech development while also safeguarding individual rights.

The rapid adoption of digital technologies in Pakistan has created pressing ethical challenges, from mass surveillance, data privacy violations, algorithmic bias to deepening socio-economic inequality. These risks are compounded by the absence of recent laws that would regulate them, enabling unimpeded governmental and corporate surveillance; biased AI systems; and unequal access to digital services. In the absence of a balanced approach that aligns technological advancements with ethical principles, Pakistan finds itself increasingly vulnerable to threats to civil liberties, social justice and equitable development. The comprehensive policy

solutions and enforceable ethical principles are needed urgently to maximize the positive potential of digital technologies, while minimizing the negative impact on society, and safeguarding the fundamental rights of citizens.

II. Methodology

This research employs an exploratory design using descriptive methods with secondary data analysis as its appropriate method. The research design would focus on analyzing existing documents such as academic works together with legal case reports legal documents and public policy materials in the field of digital ethics and justice. An evaluation of scholarly work combined with online forum materials and media reports would disclose new ethical matters appearing within digital platforms thereby including issues about privacy protection and algorithmic discrimination and digital site governance standards. A comparative study between international standards and policies about digital justice serves to demonstrate alternative methods for digital-era ethical management. The study design enables researcher to gain full knowledge of the study without performing data collection from actual participants directly.

Privacy together with data protection have emerged as primary ethical challenges because of the digital transformation that occurred in global societies. The present era proves personal data represents a valuable asset since corporations and governments perform regular large-scale collection and analysis to monetize data without sufficient consent from individuals (Zuboff, 2019). Millions of Facebook users suffered when their personal data was used by Cambridge Analytica for political manipulation in the notorious data scandal of 2018 (Cadwalladr& Graham-Harrison, 2018). These cases demonstrate the degradation of individual privacy rights in the digital economy because users often neglect understanding the future uses of their aggregated data which gets transferred between companies for profit purposes.

The European Union maintains the GDPR as its most significant example for data protection regulation yet many nations worldwide continue without sufficient laws to protect personal information (Voigt & Von demBussche, 2017). People who lack protection under full privacy laws face exposure to misuse by corporate actors as well as state agencies. The deployment of surveillance technologies under national security pretenses by governments becomes possible in countries with minimal data protection because they violate civil liberties (Privacy International, 2020). Private corporations regularly practice data sharing through secret channels which deny users any power over their information management.

III. Results

The defense of ethical integrity across digital privacy needs more developed rules and ethical systems which form stronger protective frameworks. User understanding of data usage requires authentic informed consent that exceeds basic form declarations according to Mittelstadt (2019). Organizations handling personal

data must establish data minimization requirements as an essential practice by only accepting information that fulfills specific purpose needs. Approval for user control should be the highest priority while organizations develop straightforward privacy settings along with portable data options to let people handle their digital presence. Protective measures must exist to prevent the digital economy from worsening social disparities while protecting system trust which otherwise would harm the advantages from digital change.

Exposure of ethical concerns regarding algorithmic bias alongside discrimination arose from connecting artificial intelligence systems and machine learning technology to critical management processes throughout hiring and loan approval procedures and criminal sentencing functions. AI systems which people view as neutral and unbiased transform into discriminatory tools because they accept historical data that contains discriminatory patterns (O'Neil, 2016). Facial recognition systems demonstrate a notable example of discrimination through higher misidentification mistakes affecting women and people of color compared to white men according to Buolamwini&Gebru (2018). System failure occurs because minorities are underrepresented in training datasets leading to inadequate performance among different demographic groups.

Biased algorithms cause problems which surpass the issues faced by facial recognition systems. AI-powered recruitment systems during the hiring process show preference for male applicants when filling technical positions because these occupations historically hired mainly men (Dastin, 2018). Predictive policing systems focus their predictive policing operations on impoverished and racially marked areas which leads to both excessive enforcement and systemic discrimination (Eubanks, 2018). Systems based on algorithms tend to preserve current inequalities when operated without proper testing and evaluation thus causing their amplification rather than their elimination.

The solution to address algorithmic bias needs various interrelated methods. Organizations need to disclose their AI system development process through transparency regarding algorithm design methods along with training data sources plus decision-making processes so others can perform checks and audits (Mehrabi et al., 2021). High-priority status should be given to proper data collection methods that establish representative training samples to enable equitable performance from AI systems across multiple demographic groups. Systems must proactively find and remedy biases throughout all steps in the data collecting and labeling operations. The organization must implement ongoing audits and tests for fairness as part of mandatory procedures under independent oversight to evaluate inequities affecting special populations (Raji et al., 2020).

The entire AI development should adopt principles of fairness alongside accountability and inclusivity to create ethical AI designs. The fairness metrics demographic parity and equalized odds enable quantification and reduction of biases

which appear in algorithmic outputs (Barocas&Selbst, 2016). Automated systems need well-defined accountability structures which establish algorithmic decision accountability and protective measures to enable affected people to pursue unjust outcomes. The implementation of ethical AI systems requires diverse stakeholders participation including ethicists as well as social scientists together with representatives from affected communities who must take part during both development and deployment stages to ensure complete ethical consideration (Crawford, 2021). Inadequate algorithms management protections generate an ongoing danger which leads to social inequality growth and reduces trust in artificial intelligence systems. Local governments and technology experts need to collaborate with civil society groups for creating firm regulatory frameworks that will add equity and accountability to AI tools to make them beneficial instruments of justice.

Modern society faces major challenges because limited technology access creates and expands socioeconomic and social inequalities. Modern digital technology has reshaped education and work opportunities together with communication methods but rural people alongside low-income communities, developing nations confront obstacles when accessing stable internet services and current electronic devices. When people lack access to technology, they become excluded from complete participation in the digital economy which blocks their chance to utilize online education and work remotely and participate in civic activities. The absence of digital resources creates new forms of inequality because people who lack connection to technology face permanent exclusion from modern advancements according to Van Dijk (2020).

Warschauer (2004) emphasizes that merely providing infrastructure is insufficient; users must also develop the skills to navigate digital tools. Ethical considerations play a crucial role in this process, as technological advancements should aim to reduce rather than exacerbate inequality. Policymakers and tech companies must prioritize inclusive growth, ensuring that innovations benefit all segments of society. Without deliberate efforts to bridge the digital divide, technological progress risks leaving behind the most vulnerable populations, deepening societal inequities. Therefore, a combination of infrastructure development, education, and ethical governance is necessary to create a more equitable digital future.

Warschauer (2004) demonstrates that delivering infrastructure alone is insufficient since users need digital tool navigation capabilities. The process requires ethical examination because new technology needs to help close gaps instead of making them worse. Technology leaders together with regulators need to produce plans for inclusive digital development that generates positive outcomes for all population sectors. Deliberate initiatives to eliminate digital discrepancies are fundamental because technological progress puts at risk the most disadvantaged populations who remain isolated by the digital divide thus deepening existing inequalities.

GDPR represents one of the most extensive data privacy frameworks by requiring organizations to ensure strict requirements in privacy and consent as well as transparency (European Parliament & Council of the European Union, 2016). The GDPR has sparked international policy reforms across the globe where Brazil follows with LGPD while South Africa implements POPIA. Organizations under these regulations must achieve user consent explicitly for personal data collection and must enable data requests for forgetting from their users (European Parliament & Council of the European Union, 2016, Art. 17).

Algorithms now stand as an essential point of attention for justice systems because of their accountability requirements. According to the UN Guiding Principles on Business and Human Rights (United Nations, 2011) organizations should verify that their technologies avoid discriminatory practices. AI-driven hiring solutions have revealed a systematic disadvantage against women and minority candidates in the employment process according to Buolamwini and Gebru (2018). The OECD AI Principles (2019) propose solutions for automated decision-making which include ensuring it remains fair and transparent alongside human oversight. Under the EU Artificial Intelligence Act (European Commission, 2021) multiple AI applications undergo regulatory audits according to their assessed levels of risk while banned applications fall outside of permitted use.

The use of digital surveillance raises justice issues that most intensively affect authoritarian countries since their facial recognition and predictive policing systems violate civil liberties. The International Covenant on Civil and Political Rights (ICCPR) (United Nations, 1966) contains protection provisions regarding privacy in its article 17) and prohibits arbitrary state surveillance. The implementation of China's Social Credit System triggers concerns from human rights advocates about its inconsistent enforcement (Creemers 2018). The Global Privacy Assembly (formerly International Conference of Data Protection Commissioners) works to establish worldwide privacy enforcement as an organization dedicated to digital rights protection across borders.

The implementation of universal internet access requires immediate action because it is identified as necessary for achieving UN Sustainable Development Goals (SDGs) especially SDG 9 (Industry, Innovation and Infrastructure). The reliable broadband access reaches only 53% of worldwide population according to data from International Telecommunication Union [ITU] (2021). Microsoft proposed the Digital Geneva Convention (Smith, 2017) which presents security standards to shield civilians against cyber-attacks yet countries have so far failed to establish formal binding conventions.

The digital environment of Pakistan creates specific obstacles for justice-oriented legal structures and policies while the country balances technological progress against safeguarding fundamental rights. The Prevention of Electronic Crimes Act (PECA) 2016 functions as Pakistan's main cybercrime law while

containing clauses to penalize instances of unauthorized data access (Section 3) and cyberterrorism (Section 10) together with online harassment (Section 20) (National Assembly of Pakistan, 2016). Human rights organizations express concern about PECA due to its comprehensive nature which suppresses freedom of speech because of its controversial defamation legislation (Article 19, 2021). Section 37 of the law provides the Pakistan Telecommunication Authority (PTA) with the power to block content against "glory of Islam or integrity, security or defense of Pakistan" (Digital Rights Foundation, 2022).

The current state of data protection in Pakistan exists behind more developed data protection standards which include the GDPR. The Personal Data Protection Bill received its draft during 2023 but its operational initiation remains delayed leading to citizen exposure to privacy risks (Ministry of Information Technology & Telecommunication, 2023). The lack of full data localization requirements in Pakistan creates difficulties with data transfer standards between the country and neighboring India which hampers international data flow processes (Qazi, 2022).

The modern digital legal system of Pakistan fails to meet global human rights and technological governance benchmarks during evaluation. The GDPR implements user consent requirements along with data minimization standards and right to erasure standards (European Parliament & Council of the European Union, 2016) yet the Personal Data Protection Bill (2023) in Pakistan has not taken effect leaving personal data exposed to exploitation (Ministry of IT & Telecommunication, 2023). The new draft law produced by Pakistan lacks stringent accountability mechanisms because it fails to establish independent oversight bodies and provides no clear penalties for violations which create challenges in enforcing its provisions (Digital Rights Foundation, 2023).

The wording of Section 20 in Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 allows the government to frequently silence critical voices through arbitrary arrests of journalists and activists. Section 20 of PECA establishes criminal penalties for "malicious" online material with unclear criteria which results in frequent arrests of journalists together with activists (Human Rights Watch, 2022). The Digital Services Act of the EU (2022) achieves content moderation goals along with protections of free speech which the PECA fails to provide through its harsh punitive methods.

On surveillance and privacy, the Judgment in Big Brother Watch v. The Big Brother Watch v. UK (2021) decision by the European Court of Human Rights requires states to maintain proportional surveillance guidelines yet Pakistan has no restrictions on data interception through its Fair Trial Act (2013) according to Privacy International (2022). The Federal Investigation Agency (FIA) collects citizens' data on a regular basis through PECA Section 34 since this subsection fails to implement necessary standards for proportionality and necessity as defined by the UN Principles on Counter-Terrorism and Human Rights (2021).

The digital laws of Pakistan fail to uphold fundamental rights according to both local constitutional criteria and international standards while protecting rights in digital spaces. The Prevention of Electronic Crimes Act 2016 contains extensive regulations which endanger Article 19A protection for free speech in Pakistan's constitution. The ambiguous nature of Section 20 within PECA enables authorities to prosecute emotionally critical journalists along with activists and daily users who express criticism through online content.

This poorly defined legislative framework discourages free expression demonstrations since authorities have used it multiple times to shut down critics according to recorded instances. Citywide internet content blocking requires minimal justification from Pakistan Telecommunication Authority (PTA) under PECA Section 37 which empowers them to act without proper oversight and clarity about censoring content that potentially threatens Islam and Pakistan's national identity. General Comment No. 34 from the UN Human Rights Committee presents guidelines which oppose the legal standards in Pakistan because it defines precise definitions and recognizes democratic necessity within speech restrictions. The nature of this legal clash emerges because Pakistan endorses constitutional freedoms while executing sweeping cyber regulations that breach these freedoms in every instance.

The prolonged development of data protection frameworks in Pakistan has resulted in extensive failure of this legislation. The international community including Europe through GDPR in 2016 alongside Brazil and South Africa implemented data protection frameworks yet Pakistan took a 9-year span from neglect before introducing its Personal Data Protection Bill in 2023. The absence of protective data legislation in Pakistan resulted in ongoing privacy breaches against citizens because the country did not pass such legislation during its digital development period. The newest draft law fails to fulfill international data protection criteria while it was released during the year 2023. The draft law does not maintain GDPR standards since it eliminates the investigatory powers and enforcement capabilities of independent data protection authorities in charge of regulatory enforcement.

The Pakistani version of the proposed regulatory body faces independence issues because it exists under government oversight. The absence of clear guidelines and notification requirements regarding data protection in international transfers and sensitive personal information protection methods makes the bill deficient in providing adequate standards. As Pakistan grows its digital economy the situation becomes worse because millions of people report data breaches. Inadequate data management by state entities and private organizations enables excessive and unmonitored data sharing of personal information between various entities.

Presidential policies about internet governance and digital rights in Pakistan establish severe judicial issues that destroy constitutional principles by institutional means. During JibranNasir v. Federation of Pakistan the Islamabad High Court delivered an important judicial ruling. Federation of Pakistan during 2021. Federation

of Pakistan established a 2021 court ruling that banned internet shutdowns while Pakistani authorities continue to suspend internet access throughout different parts of the country. The government of Pakistan initiated internet service stoppages in 15 incidents across Balochistan province and ex-FATA territory in addition to events such as political protests and security operations during 2022. The imposed internet shutdowns exceed national constitutional protection boundaries to breach human rights outlined in United Nations Human Rights Council resolutions regarding internet access.

The judiciary maintains inconsistent patterns for digital rights protection because judges fail to establish unique criteria during internet speech and surveillance practice case reviews. Digital rights advancements exist in limited numbers at superior courts yet lower courts mostly implement strict cyber laws through heavy enforcement. The unpredictable performance of judges creates unclear laws which give executive officials freedom to escalate their digital oversight. The lack of both dedicated digital rights courts and cyber law expertise prevents Pakistan from solving its emerging problems in digital law management and interpretation of legal standards. Citizens face extensive difficulties regarding digital rights violations because Pakistan lacks both digital rights protection agencies and cyber courts.

Digital governance in Pakistan requires better monitoring of corporate entities within its framework. The data protection system in Pakistan contains few obligations beyond those implemented in both the Consumer Privacy Act (CCPA) of California and the General Data Protection Regulation (GDPR) of the EU. Employed companies throughout Pakistan do not need to reveal their data breaches which keeps millions of users ignorant about their security incidents.

The e-commerce field and social media platforms operate without established regulations to guard consumer transactions and these platforms have no mandatory rules for their content management policies or member blocking methods. Without regulatory frameworks Pakistani technology businesses alongside international tech companies enjoy freedoms to violate user privacy standards in conjunction with ethical decisions when working in Pakistan. Private organizations together with government institutions face significant concerns due to current artificial intelligence system practices with automated decision-making tools. The proposed EU Artificial Intelligence Act provides accountability standards for algorithms which Pakistani citizens need to protect themselves from possible discriminatory actions by untraceable AI systems used in credit scoring and hiring procedures and law enforcement operations.

IV. Discussion

Research establishes critical inconsistencies that occur between Pakistan's digital laws and local constitutional rights and global human rights conventions. the main law in Pakistan regarding the cyber law known as Prevention of Electronic

Crimes Act (PECA) 2016 functions to limit free speech instead of safeguarding digital rights because it contains ambiguous articles that enable officials to restrict journalists and other Pakistani citizens through erratic censorship and charges.

The Digital Services Act framework of the EU serves as an appropriate example since it combines rules for free expression protection with content restriction measures. The Personal Data Protection Bill of Pakistan exhibits significant data protection failures since it lacks complete GDPR-level safeguards for independent oversight bodies and user rights and data transfer standards. The ongoing internet shutdowns in Pakistan continue to inflict harm despite judicial rulings that declared such measures unconstitutional thus proving executive government refusal to safeguard constitutional rights and human rights standards.

Pakistani citizens remain unable to gain substantial protection for data exploitation conducted by governments and private actors due to the absence of corporate oversight structures. The state-operated websites attest to their preference for controlling rights rather than respecting them because their institutional framework proves incapable of stopping such abuses. Multiple systematic failures issue from these underlying weaknesses which has created digital fear and reduced technical innovation as well as diminished network reliability in Pakistan. The digital rights protection standards in Pakistan lag behind contemporary global advancements thus rendering the country's approach violation of modern democratic norms. Legal system reform in Pakistan needs to become strong and sophisticated because current digital policies violate both national rights guarantees and international human rights requirements. PECA needs modification to simplify its extensive wording and Pakistan needs to create an independent data security institution responsible for digital rights law enforcement including specialized courts to resolve disputes.

Conclusion

The digital governance framework of Pakistan currently fails to protect fundamental rights and digital era ethical norms because its cyber laws restrict freedom while its data protection is weak and surveillance is widespread and persistent digital inequalities exist. Privacy protection together with expression rights protection and algorithm fairness show serious flaws worldwide yet Pakistan implements various regulations that break constitutional boundaries inconsistently. Pakistan needs to promote rapid legal framework upgrades to establish regulations that match international human rights specifications along with an independent oversight presence while ensuring political participation that integrates progress with the implementation of fundamental reforms will enable Pakistan to develop digital progress that serves all citizens as it safeguards democratic principles as well as ethical conduct during the digital era.

Bibliography

Access Now. (2023). The state of internet shutdowns in 2022. https://www.accessnow.org

Amnesty International. (2023). Automated Harassment: Facial Recognition in Pakistan. https://www.amnesty.org

Article 19. (2021). Pakistan: Overbroad and vague cybercrime law used to silence critics. https://www.article19.org

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W. W. Norton & Company.

Buolamwini, J., & Gebru, T. (2018). "*Gender shades: Intersectional accuracy disparities in commercial gender classification*." Proceedings of the Conference on Fairness, Accountability, and Transparency, 77–91.

Buolamwini, J., & Gebru, T. (2018). *Gender shades: Intersectional accuracy disparities in commercial gender classification*. Proceedings of the Conference on Fairness, Accountability, and Transparency, 77–91. https://doi.org/10.1145/3178876.3186038

Cadwalladr, C., & Graham-Harrison, E. (2018). "*Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*." The Guardian.

Creemers, R. (2018). China's social credit system: An evolving practice of control. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3175792

Digital Rights Foundation. (2022). Annual report on state of digital rights in Pakistan. https://digitalrightsfoundation.pk

European Commission. (2021). Proposal for a regulation on artificial intelligence. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

European Commission. (2021). Proposal for a regulation on artificial intelligence.

European Parliament & Council of the European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679.

European Parliament & Council of the European Union. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. https://gdpr-info.eu

Floridi, L. (2018). "Soft ethics and the governance of the digital." *Philosophy & Technology*, 31(1), 1–8.

Human Rights Watch. (2022). Silenced Dissent: PECA's Chilling Effect in Pakistan. https://www.hrw.org

International Telecommunication Union. (2021). Measuring digital development: Facts and figures. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

Media Matters for Democracy. (2023). AI Governance Gap in Pakistan. https://mediamatters.pk

Microsoft. (2022). Responsible AI principles.

Ministry of Information Technology & Telecommunication. (2023). Personal Data Protection Bill. Government of Pakistan.

National Assembly of Pakistan. (2016). Prevention of Electronic Crimes Act. Act No. XL of 2016.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens*

democracy. Crown.

OECD. (2019). OECD principles on artificial intelligence. https://www.oecd.org/ai/ai-principles

Pakistan Computer Emergency Response Team. (2021). National cybersecurity policy. https://www.pakcert.org

Qazi, U. (2022). Comparative analysis of data protection laws in South Asia. Pakistan *Journal of Law and Society*, 14(2), 45-67.

Rawls, J. (1971). *A theory of justice*. Harvard University Press.

Senate Standing Committee on IT. (2023). Proceedings on digital rights authority. Parliament of Pakistan.

Smith, B. (2017). The need for a Digital Geneva Convention. Microsoft. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

United Nations. (1966). International Covenant on Civil and Political Rights.

United Nations. (1966). International Covenant on Civil and Political Rights. https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

United Nations. (2011). Guiding Principles on Business and Human Rights. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

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