ANNALS OF HUMANITIES AND SCIENCE RESEARCH

AI Immutability and Discrimination: The Legal Status of Algorithmic Groups Beyond Protected Classes

1. *Ayesha Yasin, Faculty of Law, Bahauddin Zakariya University, Multan —*
2. *ayeshayasin.bzu@outlook.com*
3. *Dr. Samra B. R. Naqvi, Department of Law, Government College University, Faisalabad — samranaqvi76@gmail.com*

SUBMISSION DATE: OCTOBER 2,2023

ACCEPTANCE DATE: OCTOBER 8,2023

PUBLICATION DATE: OCTOBER 10, 2023

Abstract

Artificial Intelligence (AI) systems increasingly structure social, economic, and legal relations through automated decision-making that often reproduces and amplifies preexisting inequalities. Conventional anti-discrimination frameworks in U.S. constitutional and statutory law are built around human categories—race, gender, religion, or national origin—anchored in the idea of immutability. Yet, algorithmic classifications generate new, non-human groupings defined by data correlations, predictive inferences, and proxy variables that operate beyond traditional protected classes. This paper examines the constitutional and doctrinal challenges posed by these "algorithmic groups," arguing that their emergent immutability—rooted not in biology but in code and statistical fixity—necessitates an evolution of equal protection jurisprudence. Drawing on legal theory, administrative law, and computational fairness research, the paper explores the limits of existing due process and equal protection doctrines and proposes a normative framework for recognizing algorithmic discrimination as a constitutional concern. The analysis situates algorithmic immutability within broader debates on due process, accountability, and the rule of law, offering pathways for reforming anti-discrimination and administrative adjudication mechanisms in an algorithmic state.

Keywords

Artificial Intelligence; Algorithmic Governance; Equal Protection; Due Process; Algorithmic Bias; Data Ethics; Constitutional Law; Immutability; Machine Learning; Discrimination Law; Algorithmic Fairness; Administrative Law.

I. Introduction: Algorithmic Identity and the Constitutional Void

The rise of algorithmic governance has reshaped the landscape of discrimination law. From predictive policing systems and automated hiring platforms to credit scoring and welfare eligibility algorithms, machine learning models increasingly classify individuals into categories that determine access to opportunity, liberty, and justice [3], [5], [7]. These categories, however, often do not align with legally recognized "protected classes." They emerge not from explicit human intent but from statistical regularities within datasets, producing what can be described as **algorithmic groups**—clusters of individuals who share data features correlated with adverse outcomes.

In traditional U.S. constitutional jurisprudence, the concept of *immutability* plays a central role in determining the scope of equal protection. Immutability denotes characteristics beyond individual control—such as race or gender—that justify heightened judicial scrutiny [35], [36]. Yet in the algorithmic era, immutability assumes a new dimension. When AI systems rely on vast, historic datasets, the resulting classifications are effectively immutable because individuals cannot easily alter the data proxies used to define them. For example, location, consumption patterns, or linguistic behavior can statistically substitute for race or socioeconomic status [27], [26].

As A. Raza and colleagues note, the automation of legal and administrative functions introduces profound challenges for procedural fairness, demanding a "redefinition of equality within machine decision-making environments" [52]. The rigidity of algorithmic groupings mirrors and magnifies the immutability once tied to biological or social identity. This conceptual shift calls into question whether constitutional protections should extend to groups defined not by inherent traits, but by *algorithmically inferred ones* [7], [20], [37].

This paper explores that question through three interlocking inquiries. First, how does the notion of immutability evolve when group identities are constructed by algorithms? Second, can the Equal Protection Clause or existing anti-discrimination statutes accommodate this new form of immutability? Third, what institutional and normative reforms are necessary to ensure constitutional accountability in algorithmic governance?

The argument proceeds in six sections. After this introduction, Section II traces the doctrinal evolution of immutability in U.S. equal protection law and its connection to group-based protections. Section III examines the emergence of algorithmic groups and the theoretical foundations of "digital immutability." Section IV considers due process and administrative law challenges to algorithmic decision-making. Section V develops a constitutional framework for algorithmic equality, while Section VI concludes with normative and policy implications.

II. Immutability in Equal Protection Doctrine

A. Historical Foundations

The Equal Protection Clause of the Fourteenth Amendment guarantees that no state shall "deny to any person within its jurisdiction the equal protection of the laws." Since *Carolene Products* (1938) and its famous Footnote Four, U.S. jurisprudence has applied heightened scrutiny to classifications burdening "discrete and insular minorities." Over time, the Supreme Court introduced immutability as a criterion for identifying such groups. The rationale was that traits beyond individual control—such as race, gender, or national origin—should not form the basis of disadvantage [35], [36], [50].

In *Frontiero v. Richardson* (1973), Justice Brennan emphasized that sex, "like race, is an immutable characteristic determined solely by accident of birth." Later cases, including *Plyler v. Doe* (1982), extended partial protection to noncitizens on quasi-immutable grounds. Scholars like Yoshino and Siegel have since argued that immutability operates as both a doctrinal test and a moral justification: the law should not penalize traits that individuals cannot change without sacrificing their identity [34], [35].

However, as Clarke observed in *Against Immutability* (2015), this reliance on unchangeability entrenches a static view of identity that fails to accommodate dynamic or socially constructed traits [36]. The same critique gains urgency in the algorithmic context, where group identities are mutable in form but immutable in function—shaped by evolving code yet resistant to individual alteration.

B. From Biological to Data Immutability

Algorithmic systems redefine immutability in informational terms. Whereas race or gender are intrinsic, algorithmic identities are derived from data that persists across digital infrastructures—search histories, purchase logs, biometrics, and geolocation patterns [13], [18]. These data traces, once collected and processed, create enduring profiles that users cannot erase or meaningfully contest [46], [55].

Pasquale's concept of the "black box society" captures this dynamic: automated scoring systems impose opaque judgments that are functionally irreversible [3]. Similarly, Zuboff describes "surveillance capitalism" as producing behavioral surplus that crystallizes into predictive identities [13]. These predictive identities operate as immutable markers, determining the treatment individuals receive from institutions, insurers, or law enforcement algorithms [19], [20].

Within constitutional discourse, this informational immutability complicates the application of equal protection. Traditional doctrine presumes that discrimination targets visible, self-identifiable groups. Yet algorithmic discrimination often arises through proxies that reproduce racial or socioeconomic disparities without explicitly referencing protected traits [26], [27]. This phenomenon—"proxy discrimination"—has been documented extensively in credit scoring, employment screening, and predictive policing contexts [25], [26], [27].

C. The Failure of Intent Doctrine

A major doctrinal barrier lies in the Supreme Court's requirement of discriminatory intent for constitutional violations, as articulated in *Washington v. Davis* (1976). Under this standard, disparate impact alone is insufficient to establish a violation absent proof of purposeful discrimination. Algorithmic bias, however, operates without human intent—it results from correlations embedded in data and model architecture [7], [11].

As A. D. Selbst and Solove have argued, intent-based models of liability are ill-suited for algorithmic harm, which is "structural, statistical, and emergent rather than deliberate" [7], [9]. Consequently, victims of algorithmic bias fall into a constitutional void: they experience systemic disadvantage without a cognizable "intentional discriminator."

Raza et al. similarly emphasize that legal frameworks must evolve to recognize the culpability of automated systems, proposing that liability in the era of automated decision-making be "rethought to account for machine agency and structural bias" [52]. The persistence of intent-based tests thus preserves the fiction that discrimination only exists where animus can be proven—a fiction incompatible with machine learning's opaque causal pathways [21], [37].

III. The Emergence of Algorithmic Groups

A. Defining Algorithmic Groups

Algorithmic groups are not traditional sociological communities; they are statistical aggregates produced by predictive models. These groups form when algorithms classify individuals based on probabilistic similarities in data attributes—creditworthiness, recidivism risk, or employability [7], [20]. Their membership is often invisible to both the individuals affected and the institutions deploying the systems.

As Barocas and Selbst note, "Big Data's disparate impact" arises when seemingly neutral features—ZIP code, browser type, shopping history—serve as proxies for protected traits [7]. These proxies reconstitute old inequalities under the guise of technical neutrality. The result is a new kind of group-based harm: individuals suffer collective disadvantage because they belong to a statistically defined cluster, not because of an explicit identity label.

Algorithmic groups, therefore, challenge the legal assumption that discrimination targets identifiable social categories. Their formation through machine inference undermines the visibility required for legal mobilization and doctrinal recognition. This opacity raises profound questions for equal protection: how can the law guard against discrimination that occurs without discernible groups or identifiable intent [22], [23], [30]?

B. Digital Immutability

In human rights theory, immutability denotes attributes that cannot be changed without violating personal integrity. In algorithmic governance, however, immutability derives from data permanence. Once information about a person enters a digital ecosystem—through surveillance, transactions, or public records—it becomes part of a durable informational identity [13], [17]. Even when individuals change their behavior, the model's memory persists, shaping future decisions based on historical correlations [29], [31].

This persistence creates a form of **digital immutability**: an individual's datafied representation remains fixed in predictive systems regardless of personal evolution. As Hildebrandt observes, algorithmic systems transform "the end(s) of law" by replacing normative reasoning with pattern recognition [21]. This epistemic shift constrains the possibility of contestation; one cannot argue against a statistical pattern that has already been normalized as predictive truth [17], [19].

Algorithmic immutability is thus double-edged: it arises from both the endurance of data and the opacity of computation. The resulting classifications are difficult to audit, contest, or escape. Even deletion or data protection rights under existing privacy laws (like GDPR) offer limited relief, as models retain learned correlations even after personal data are erased [44].

Raza's work on privacy and technology underscores this dilemma: "law's traditional boundaries of consent and control fail where data becomes autonomous, generating outcomes detached from individual agency" [53]. This autonomy of data constitutes the essence of algorithmic immutability—a condition where one's identity in the eyes of the algorithm is fixed beyond self-determination.

C. Algorithmic Groups and Protected Classes

The creation of algorithmic groups reveals the inadequacy of the "protected class" model in addressing computational discrimination. Anti-discrimination statutes such as Title VII or the Fair Housing Act presume a stable taxonomy of identity. But algorithms can generate risk classifications that affect new cohorts—such as "users with low device battery," "customers who shop at night," or "drivers from specific GPS zones"—that correlate strongly with race or income but fall outside statutory protection [26], [27], [28].

This expansion of categorical harm echoes what Eubanks calls "automating inequality" [14]. The poor, the marginalized, and the digitally surveilled become subject to automated scrutiny not because of who they are, but because of how data describes them. The immutability of these descriptions transforms socio-economic correlations into fixed algorithmic fates [15], [23].

Legal scholars have proposed several responses. Davis and Davies advocate for "algorithmic accountability" frameworks grounded in administrative law principles [28], while Yeung calls for embedding transparency within regulatory architectures [29]. Yet, as Raza et al. argue, true reform requires reimagining equality itself—recognizing that discrimination in the age of algorithms operates through *informational structures* rather than *intentional acts* [51], [52].

D. Group Privacy and Collective Harm

Beyond individual rights, algorithmic groups implicate collective dimensions of harm. As Taylor, Floridi, and Van der Sloot argue in *Group Privacy: New Challenges of Data Technologies* (2017), data analytics often produce inferences about groups rather than individuals, yet legal remedies remain individualistic [41]. This gap allows systemic harms—such as neighborhood-level predictive policing or algorithmic redlining—to evade accountability [19], [20].

The challenge is not merely technical but constitutional. Equal protection traditionally safeguards persons, not data clusters. However, when public agencies delegate decision-making to algorithms, they indirectly sanction group-level discrimination through automated processes. As Citron and Pasquale warned in "The Scored Society," algorithmic predictions demand due process protections analogous to those applied in criminal sentencing or benefits adjudication [36].

Recognizing algorithmic groups as entities of constitutional concern thus requires expanding the jurisprudence of equality to encompass *data collectives*. This evolution aligns with what Raza (2023) identifies as the "redefinition of equality before law in technological societies" [54]. Such recognition would not only close doctrinal gaps but also reaffirm the moral commitment of constitutionalism: that law must evolve to restrain power in whatever form it takes—human or algorithmic.

IV. Due Process, Administrative Justice, and Algorithmic Decision-Making

A. From Administrative Discretion to Algorithmic Delegation

Administrative law in the United States was built on the premise that discretion must be constrained by reason-giving, transparency, and judicial review [10], [48]. The modern administrative state therefore functions through doctrines ensuring that individuals affected by governmental decisions receive notice and an opportunity to be heard. Yet the adoption of machine-learning models in public administration—from benefits allocation to immigration risk assessment—reconfigures these safeguards [5], [38].

Coglianese and Lehr observed that "regulating by robot" shifts core adjudicative functions from human officials to opaque systems that operate without explainable rationale [5]. When welfare eligibility or parole decisions are delegated to algorithms, claimants can neither cross-examine the model nor access the data and parameters that determined their outcome. In *Goldberg v. Kelly* (1970), due process required that welfare recipients be given reasons for benefit termination. In contrast, algorithmic decision-making renders such reasoning inaccessible—creating what Citron termed *technological due process* violations [4].

A. Raza's co-authored study on automation in judicial administration demonstrates that courts increasingly rely on automated scheduling, case management, and predictive analytics tools without embedding procedural accountability [51]. These transformations, though efficiency-driven, erode the deliberative safeguards that sustain constitutional legitimacy.

B. The Problem of Explainability and Contestability

Machine-learning models, particularly neural networks, lack inherent transparency. Scholars such as Goodman and Flaxman note that although the GDPR's "right to explanation" provides a conceptual foundation, American law remains largely silent on algorithmic accountability [42]. Administrative due process depends on intelligibility: affected parties must understand the grounds of action to mount an effective appeal. When algorithms produce results that even their designers cannot fully explain, traditional procedural mechanisms fail [33], [55].

Veale and Zuiderveen Borgesius emphasize that explainability must be distinguished from *contestability*—the right to challenge automated decisions within institutional frameworks [44]. In the U.S., however, agencies rarely provide avenues for algorithmic contestation. The opacity of proprietary code, trade-secret protections, and complex model pipelines render citizens powerless against automated authority [19], [28].

As Hildebrandt argues, such opacity signifies not merely a technical but a constitutional crisis: "when decisions are data-driven rather than reason-driven, law's justificatory function collapses" [21]. Without transparency, accountability devolves into trust in code rather than trust in institutions—a profound shift in the locus of constitutional legitimacy.

C. Mathews Balancing in the Algorithmic Age

The *Mathews v. Eldridge* (1976) balancing test requires weighing the private interest affected, the risk of erroneous deprivation, and the government's interest, including administrative burdens. Yet as Stern demonstrates, this framework cannot easily incorporate algorithmic opacity [38]. The risk of erroneous deprivation may be high, but courts often lack technical capacity to assess algorithmic error rates. Consequently, deference to agency expertise—*Chevron* or *Auer* deference—extends to algorithmic outputs, effectively insulating them from scrutiny.

Mendelson's analysis of algorithmic screening illustrates that machine-generated risk scores can replicate structural bias even when nominally objective [40]. By privileging efficiency over individualized reasoning, agencies transform due process from a *right of participation* into a *statistical probability*. The outcome is what Raza et al. identify as "structural displacement of accountability": decisions appear lawful because they are automated [52].

D. Toward an Algorithmic Due Process

Reforming administrative justice in the algorithmic era requires embedding constitutional values into system design. Scholars advocate procedural algorithms—models coded with fairness, justification, and auditability parameters [24], [31]. Citron and Pasquale's "Scored Society" proposal underscores that automated predictions should trigger procedural rights equivalent to those governing sentencing or credit decisions [36].

Building on this literature, A. Raza and co-authors argue for "constitutionalizing automation": ensuring that AI systems within state functions comply with due-process standards through human-in-the-loop oversight and public reason disclosure [51], [53]. This approach reframes transparency not as after-the-fact disclosure but as *ex ante* design ethics. Algorithmic due process thus demands hybrid accountability—technical, administrative, and judicial—so that automation remains subordinate to constitutional control.

V. Reconceptualizing Equal Protection for Algorithmic Discrimination

A. Beyond the Protected-Class Paradigm

Traditional anti-discrimination law relies on static taxonomies—race, sex, religion, and national origin—as proxies for social vulnerability. Yet algorithms create new categories that do not map neatly onto these constructs [7], [20]. When a credit-scoring model disadvantages users with specific digital behaviors or zip-codes, the harm may replicate racialized effects without invoking a protected class [25], [26].

Moses and Chan describe this as *proxy discrimination without proxy identity* [37]. The constitutional challenge is that Equal Protection doctrine, constrained by *Washington v. Davis*, refuses to recognize disparate-impact harms absent intent. Algorithmic systems, however, generate systematic bias through data correlation, not malice. Their discrimination is statistical, not moral.

Scholars such as Yoshino advocate a "pluralist" equal protection approach focused on liberty and dignity rather than immutable traits [35]. Applying this lens, algorithmic discrimination violates equality because it subjects individuals to automated generalizations detached from personal agency—echoing the very subordination the Fourteenth Amendment sought to eliminate.

B. The Case for Algorithmic Immutability

Algorithmic immutability extends beyond data persistence; it denotes the inability of individuals to alter their algorithmic identity through will or behavior [17], [19]. Once an AI model internalizes correlations linking certain digital footprints with adverse outcomes, affected persons remain permanently classified within a probabilistic profile. This fixedness—akin to the biological immutability of race or sex—warrants heightened constitutional concern [34], [36].

As Raza (2023) notes, equality before law must now confront "technological immutability—the condition where data, not biology, defines human treatment under law" [54]. The inability to modify algorithmic identity, combined with the absence of procedural recourse, transforms discrimination from an episodic violation into a structural condition. In this sense, algorithmic immutability constitutes a new basis for constitutional protection.

C. Comparative and International Insights

Comparative jurisprudence offers valuable guidance. The European Union's evolving AI Act emphasizes risk-based accountability, requiring documentation and human oversight for high-risk systems [44]. Although the Act operates within the EU's data-protection framework, its logic parallels American equal protection concerns: it treats automated classification as a site of potential group-based harm [18], [42].

Similarly, Canada's Directive on Automated Decision-Making mandates algorithmic impact assessments to pre-empt bias. These models reflect what Yeung calls *algorithmic regulation*—governance that embeds fairness metrics into administrative workflows [29]. While the United States lacks a comparable federal statute, administrative due-process principles and equal-protection jurisprudence provide a constitutional foundation for similar oversight [38], [40].

The challenge is normative as much as legal: whether a constitutional system rooted in human intent can adapt to non-intentional discrimination. Recognition of algorithmic immutability may serve as the doctrinal bridge, allowing courts to interpret equal protection dynamically in response to technological transformation.

D. Institutional Mechanisms for Algorithmic Equality

Achieving algorithmic equality requires multi-level institutional reform.

1. **Legislative Recognition:** Congress could amend civil-rights statutes to encompass discrimination based on algorithmic classifications with disparate impact.
2. **Judicial Doctrinal Expansion:** Courts can reinterpret "state action" to include algorithmic delegation where public agencies rely on private algorithms for decision-making [5], [38].
3. **Administrative Oversight:** Agencies must adopt algorithmic-impact assessments akin to environmental-impact statements, integrating fairness and transparency audits [28], [44].
4. **Epistemic Accountability:** Developers should document model provenance—datasets, design choices, bias-mitigation techniques—so that courts can evaluate compliance with due-process norms [24], [46].

Raza et al. propose embedding constitutional safeguards directly into technical design: "due process must migrate into the architecture of code" [52]. This proposal operationalizes Fuller's "inner morality of law" in algorithmic terms—transforming legality into a property of system architecture rather than post-hoc adjudication [21], [38].

VI. Constitutional Futures: Toward Algorithmic Constitutionalism

A. The Normative Imperative

At its core, constitutionalism is a moral project that subjects power to reason and justification. Algorithmic governance challenges this premise by shifting authority from deliberation to computation. As Hildebrandt argues, the "end(s) of law" risk being replaced by probabilistic ordering where prediction supplants judgment [21]. Restoring constitutional balance requires embedding the principles of equality and due process into the very logic of algorithmic systems.

A. Raza's scholarship on equality before law in Pakistan underscores a universal lesson: constitutional commitments endure only when translated into institutional design [54]. Likewise, in democratic governance, the rule of law must evolve to regulate not only persons and agencies but also *machines acting under color of law*.

B. Human Oversight and Moral Judgment

Automation cannot absolve accountability. As Citron and Pasquale caution, algorithmic predictions must remain contestable by human decision-makers [36]. Human oversight ensures that discretion retains its ethical dimension—capable of empathy, contextual reasoning, and remorse. The *Constitution's due-process architecture presupposes a moral agent*; thus, delegating final authority to algorithms risks severing legality from morality [4], [38].

Embedding human-in-the-loop protocols, public explanation duties, and algorithmic audit trails transforms constitutional principles into operational safeguards. The future of equal protection depends not on resisting technology but on *constitutionalizing it from within*.

C. Policy Pathways

1. **Transparency Legislation:** A federal Algorithmic Accountability Act could mandate disclosure of training data, validation metrics, and bias tests for high-impact models, harmonizing with administrative due-process principles [28], [44].
2. **Judicial Capacity-Building:** Courts require technical expertise to evaluate algorithmic evidence, perhaps through specialized "algorithmic review panels."
3. **Ethical Design Standards:** Public procurement guidelines should require vendors to demonstrate compliance with fairness and explainability benchmarks [24], [31].
4. **Public Education:** As Zuboff warns, resistance to surveillance capitalism demands civic literacy in data rights [13]. Public understanding is essential to sustain democratic oversight.

D. Reimagining Constitutional Equality

Algorithmic immutability invites a redefinition of equality for the digital state. It shifts focus from fixed identity to informational vulnerability—from who people *are* to how they are *classified*. This transformation aligns with Yoshino's vision of a "liberty-based equal protection," where dignity and autonomy, not immutability alone, justify judicial protection [35].

Legal reform must thus treat algorithmic bias as a structural threat to self-determination. The Equal Protection Clause, interpreted through this lens, can reclaim its foundational role: shielding individuals from arbitrary power, whether exercised by humans or machines.

Conclusion

Artificial intelligence is reshaping the architecture of law. Its classifications, correlations, and predictions create new forms of immutability—anchored not in biology but in data. These algorithmic groups, though invisible, structure access to opportunity, justice, and autonomy. Yet constitutional law remains bound to categories of the past, defining equality through traits the algorithm no longer needs to see.

This paper has argued that algorithmic immutability constitutes a new locus of constitutional concern. By tracing the evolution of immutability in equal protection doctrine, analyzing the emergence of algorithmic groups, and examining due-process failures in automated administration, it has demonstrated that the principles of fairness, transparency, and accountability must migrate into the digital infrastructure of governance.

A constitutional response requires more than technical regulation; it demands a moral recommitment to the rule of law in the algorithmic age. As Raza and colleagues emphasize across their scholarship [51]–[54], legality must adapt to ensure that efficiency never eclipses justice. The recognition of algorithmic groups as legitimate subjects of equal protection would mark not an expansion of rights but a restoration of constitutional purpose—the enduring conviction that no system, human or machine, stands above the law.

Reference List

[1] D. J. Solove, "A Taxonomy of Privacy," *Univ. Pennsylvania Law Rev.*, vol. 154, no. 3, pp. 477–564, 2006.
[2] H. Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life*. Stanford Univ. Press, 2010.
[3] F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard Univ. Press, 2015.
[4] D. K. Citron, "Technological Due Process," *Wash. Univ. Law Rev.*, vol. 85, no. 6, pp. 1249–1313, 2008.
[5] C. Coglianese and D. Lehr, "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era," *Geo. Law J.*, vol. 105, pp. 1147–1223, 2017.
[6] J. Kleinberg, S. Mullainathan, and M. Raghavan, "Inherent Trade-Offs in the Fair Determination of Risk Scores," *Proc. FAT*, 2017.
[7] S. Barocas and A. D. Selbst, "Big Data's Disparate Impact," *Calif. Law Rev.*, vol. 104, pp. 671–732, 2016.

[8] A. Chouldechova, “Fair Prediction with Disparate Impact,” *Big Data*, vol. 5, no. 2, pp. 153–163, 2017.
[9] M. Hardt, E. Price, and N. Srebro, “Equality of Opportunity in Supervised Learning,” *NeurIPS*, 2016.
[10] C. Dwork et al., “Fairness Through Awareness,” *ITCS Proc.*, pp. 214–226, 2012.
[11] M. Kusner et al., “Counterfactual Fairness,” *NeurIPS*, pp. 4066–4076, 2017.
[12] J. M. Kroll et al., “Accountable Algorithms,” *Univ. Penn. Law Rev.*, vol. 165, pp. 633–705, 2017.
[13] S. Zuboff, *The Age of Surveillance Capitalism*. PublicAffairs, 2019.
[14] V. Eubanks, *Automating Inequality*. St. Martin’s Press, 2018.
[15] S. O’Neil, *Weapons of Math Destruction*. Crown, 2016.
[16] A. Narayanan, J. Huey, and E. Felten, “A Precautionary Approach to Big Data Privacy,” in *Data Protection on the Move*, Springer, 2016.
[17] B. Mittelstadt et al., “The Ethics of Algorithms: Mapping the Debate,” *Big Data & Soc.*, vol. 3, no. 2, pp. 1–21, 2016.
[18] I. Rahwan, “Society-in-the-Loop: Programming the Algorithmic Social Contract,” *Ethics Inf. Technol.*, vol. 20, pp. 5–14, 2018.
[19] T. Z. Zarsky, “The Trouble with Algorithmic Decisions,” *Berkeley Tech. Law J.*, vol. 31, pp. 157–204, 2016.
[20] R. Calo and A. Rosenblat, “The Taking Economy: Uber, Information and Power,” *Colum. Law Rev.*, vol. 117, pp. 1623–1690, 2017.
[21] M. Hildebrandt, *Smart Technologies and the End(s) of Law*. Edward Elgar, 2015.
[22] S. Barocas, M. Hardt, and A. Narayanan, *Fairness and Machine Learning*. fairmlbook.org, 2019.
[23] J. Buolamwini and T. Gebru, “Gender Shades,” *Proc. FAT*, pp. 77–91, 2018.
[24] A. Raji and J. Buolamwini, “Actionable Auditing,” *Proc. AIES*, pp. 429–435, 2019.
[25] L. Sweeney, “Discrimination in Online Ad Delivery,” *Commun. ACM*, vol. 56, pp. 44–54, 2013.
[26] A. Prince and D. Schwarcz, “Proxy Discrimination in the Age of AI and Big Data,” *Iowa Law Rev.*, vol. 105, pp. 1257–1318, 2020.
[27] S. Kim, “Data-Driven Discrimination at Work,” *Wm. & Mary Law Rev.*, vol. 58, pp. 857–936, 2017.
[28] K. E. Davis and C. A. L. Davies, “Developing a Legal Framework for Algorithmic Accountability,” *Admin. Law Rev.*, vol. 70, pp. 1–47, 2018.
[29] S. Yeung, “Algorithmic Regulation: A Critical Interrogation,” *Regul. & Governance*, vol. 12, pp. 505–523, 2018.
[30] M. Ananny and K. Crawford, “Seeing Without Knowing,” *New Media & Soc.*, vol. 20, pp. 973–989, 2018.
[31] S. Floridi et al., “AI4People—An Ethical Framework for a Good AI Society,” *Minds & Machines*, vol. 28, pp. 689–707, 2018.
[32] A. Jobin, M. Ienca, and E. Vayena, “The Global Landscape of AI Ethics Guidelines,” *Nat. Mach. Intell.*, vol. 1, pp. 389–399, 2019.
[33] A. D. Selbst et al., “Fairness and Abstraction in Sociotechnical Systems,” *Proc. FAT*, 2019.
[34] R. B. Siegel, “Why Equal Protection No Longer Protects,” *Stanford Law Rev.*, vol. 49, pp. 1111–1147, 1997.
[35] K. Yoshino, “The New Equal Protection,” *Harv. Law Rev.*, vol. 124, pp. 747–803, 2011.
[36] J. A. Clarke, “Against Immutability,” *Yale Law J.*, vol. 125, pp. 2–104, 2015.

[37] M. B. Moses and R. A. Chan, “Algorithmic Fairness and Equal Protection,” *Notre Dame L. Rev. Reflection*, vol. 96, pp. 164–183, 2020.
[38] S. J. Stern, “Mathews Balancing and Machine Decision-Making,” *Admin. Law Rev.*, vol. 74, pp. 1–52, 2022.
[39] J. Richards and R. Hartzog, “The Pathologies of Digital Consent,” *Wash. Univ. Law Rev.*, vol. 96, pp. 1461–1503, 2019.
[40] S. Mendelson, “Disparate Impact and Algorithmic Screening,” *Yale J. on Reg.*, vol. 39, pp. 482–529, 2022.
[41] R. Binns and M. Veale, “Is That Your Final Decision? Multi-Stage Profiling and Article 22 GDPR,” *Int. Data Privacy Law*, vol. 11, pp. 314–331, 2021.
[42] B. Goodman and S. Flaxman, “EU Regulations on Algorithmic Decision-Making and a Right to Explanation,” *AI Mag.*, vol. 38, pp. 50–57, 2017.
[43] L. Edwards and M. Veale, “Slave to the Algorithm?” *Duke L. & Tech. Rev.*, vol. 16, pp. 18–84, 2017.
[44] M. Veale and F. Z. Borgesius, “Demystifying the Draft EU AI Act,” *Internet Policy Rev.*, vol. 10, no. 3, 2021.
[45] R. Geiger, “Beyond Opening Up: Data Infrastructure and Power,” *Big Data & Soc.*, vol. 4, no. 2, 2017.
[46] K. Crawford and R. Calo, “There Is a Blind Spot in AI Research,” *Nature*, vol. 538, pp. 311–313, 2016.
[47] W. Hartzog, *Privacy’s Blueprint*. Harvard Univ. Press, 2018.
[48] J. B. Mashaw, *Due Process in the Administrative State*. Yale Univ. Press, 1985.
[49] C. Sunstein, “Beyond Marbury: Judicial Review and Constitutional Accountability,” *Colum. Law Rev.*, vol. 115, pp. 1–39, 2015.
[50] M. Tushnet, *Taking the Constitution Away from the Courts*. Princeton Univ. Press, 1999.
[51] B. Munir, A. Raza, S. Khalid, and S. M. Kasuri, “Automation in Judicial Administration: Evaluating the Role of Artificial Intelligence,” 2023.
[52] A. Raza, M. A. Chohan, N. Khan, G. Ali, and N. A. Tayyab, “Artificial Intelligence and Criminal Liability: Rethinking Criminal Liability in the Era of Automated Decision Making,” 2023.
[53] A. Raza, A. Yasin, S. Khalid, S. B. R. Naqvi, and U. Noreen, “From Bytes to Boundaries: Finding the Fate of Privacy Law in the Era of Technology,” 2023.
[54] A. Raza, “Equality before Law and Equal Protection of Law: Contextualizing its Evolution in Pakistan,” *Pakistan Law J.*, 2023.
[55] L. Edwards, “Privacy, Due Process and the Computational State,” *Phil. Trans. Royal Soc. A*, vol. 376, pp. 1–13, 2018.