



ILE

ILE JOURNAL OF GOVERNANCE AND
POLICY REVIEW

VOLUME 3 AND ISSUE 1 OF 2025

INSTITUTE OF LEGAL EDUCATION



ILE JOURNAL OF GOVERNANCE AND POLICY REVIEW

(Open Access Journal)

Journal's Home Page – <https://jgpr.ilededu.in/>

Journal's Editorial Page – <https://jgpr.ilededu.in/editorial-board/>

Volume 3 and Issue 1 (Access Full Issue on – <https://jgpr.ilededu.in/category/volume-3-and-issue-1-of-2025/>)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 – info@ilededu.in / Chairman@ilededu.in



© Institute of Legal Education

Copyright Disclaimer: All rights are reserve with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For more details refer <https://jgpr.ilededu.in/terms-and-condition/>

ALGORITHMIC GOVERNANCE AND DEMOCRATIC VALUES: EVALUATING THE IMPACT OF STATE USE OF AI ON TRANSPARENCY, ACCOUNTABILITY AND CIVIL LIBERTIES

AUTHOR - PAZHAMALAI S, FACULTY, GOVERNMENT LAW COLLEGE, TIRUCHIRAPPALLI - 620023

BEST CITATION - PAZHAMALAI S, ALGORITHMIC GOVERNANCE AND DEMOCRATIC VALUES: EVALUATING THE
IMPACT OF STATE USE OF AI ON TRANSPARENCY, ACCOUNTABILITY AND CIVIL LIBERTIES, *ILE JOURNAL OF
GOVERNANCE AND POLICY REVIEW*, 3 (1) OF 2025, PG. 30-38, APIS 3920-0032 | ISSN - 2583 - 8032. DOI -
<https://doi.org/10.65393/VWFD5839>

ABSTRACT

The rapid adoption of AI by the government for predictive policing, welfare targeting, and election administration is changing the nature of citizen-state interaction. The systems that come along with AI implementation hold the promise of improved risk management and effectiveness at the same time threatening core democratic values such as accountability, transparency, equality, and civil rights. Predictive policing is likely to be a historically biased system consequently leading to increased monitoring of and lack of protection for marginalized communities. Welfare algorithms are involved in eligibility, fraud detection, and benefit allocation. They often operate as unclear "black boxes," thus making it hard for people to understand or appeal adverse decisions and they are at the same time weakening the fairness of the process and the right to contest it. The technology of AI in elections from political ads targeting and micro-profiling to automated content moderation has the potential to subtly alter the information environment, thereby affecting voter independence and public discourse. This article looks at how such AI deployments disturb the customary channels of democratic control and supervision, claiming that the current legal and institutional settings are not capable of dealing with issues like lack of transparency in algorithms, data-driven discrimination, and distributed responsibility. It further suggests measures like algorithmic impact assessments, rights to explanation and contestation, independent audits, and high data-protection standards, arguing that the use of algorithms in governance can be justified only if it is done within a framework that protects civil liberties and ensures real accountability.

Keywords: Algorithmic governance, Predictive policing, Welfare algorithms, Election technology, Transparency and accountability, Civil liberties, Digital constitutionalism

I. INTRODUCTION:

Artificial intelligence is being implemented by governments all over the globe in basic functions like law enforcement, welfare administration, and electoral processes. The main advantages of these rollouts are efficiency and objectivity, but at the same time, the use of algorithms in governance has an inherent conflict with democracy. AI vision of policing that uses historical arrest data to

determine which neighborhoods need watchful eye and intensive surveillance, a welfare algorithm that quietly denies assistance to the needy, and electoral technology that targets voters with personalized political messages all characterize the state using power through systems that are often unclear, hard to dispute, and, at the same time, reinforce the existing discrimination due to their nature. The present article discusses the issue of algorithmic governance in three crucial spheres predictive

policing, welfare administration, and election technology as a factor that reduces transparency, disperses accountability, and impairs civil rights. Author of the article claims that current legal frameworks, made for human decision-makers functioning within hierarchical institutions, lack the ability to control algorithmic decision-making. The article ends by pointing out the essential protections: mandatory algorithmic impact assessments, rights to explanation and contestation, independent audits, and a reframed constitutional approach to algorithmic power that acknowledges both state and private actors as sources of risk to fundamental rights.

II. ALGORITHMIC GOVERNANCE ACROSS THREE DOMAINS

A. Predictive Policing - From Data-Driven Efficiency to Automated Discrimination:

Predictive policing is a clear demonstration of law enforcement agencies accepting the use of artificial intelligence in dispatching workforce to the different areas, spotting the people with a high risk of committing offenses, and thwarting the crime before it happens. The reasoning is very attractive at first glance: the police can use past crime data, advanced analytics, and geospatial mapping to target their patrols where there is a higher risk of crime and thus optimize the safety of the public given the limited resources. Nevertheless, the whole system rests on a basic error: the belief that past crime data shows the true crime patterns and not the patterns of police activity³⁰. Crime figures are not straightforward indicators of criminal activity. They stand for just those offenses that law enforcement has opted to investigate and record. In America and worldwide, authorities have always kept an eye on and enforced law in poor, non-White areas—a pattern that comes from years of redlining, residential segregation, and racialized policing. These areas, which have

police presence that is disproportionate to the actual crime rates, become the source of high arrest and conviction records³¹. When predictive algorithms analyze such data, they do not rectify historical bias; rather, they make it a part of their processing. The Strategic Subject List of Chicago, which brought historical arrest records into the picture to identify people likely to be involved in gun violence, mostly pointed fingers at Black and Latino men, most of whom had never committed any violent crime. There was no technical malfunction; it was the outcome of the very biased historical data that had been fed into an algorithm that was bound to reproduce it³².

India has a face-off with similar issues. The Status of Policing in India Report (2019) unearthed a substantial bias in police actions against Muslim populations, immigrants, and uneducated people. If the state police are going to use predictive systems that have been trained on such distorted data, these systems will necessarily have the discrimination of the past written into them and even further amplified. The Wisconsin Supreme Court in *State v. Loomis*³³ was not persuaded by a due process challenge to the COMPAS risk assessment tool, upholding that the use of such instruments was constitutional despite their taking into account factors including the defendant's sex. The reasoning of the court is a clear case of uncritical acceptance of technological objectivity the assumption that algorithms, being data-driven, just cannot be biased³⁴.

Predictive policing instigates a cycle where automated bias eventually becomes the

³⁰ Tanishka Goswami, Shikhar Aggarwal & Ayan Gupta, Predictive Policing: Discrimination, Due Process and Democratic Accountability, 39A BLOG (Mar. 23, 2022), <https://p39ablog.com/2022/03/predictive-policing-discrimination-due-process-and-democratic-accountability/>

³¹ AMNESTY INT'L & EUR. AI SOC'Y FUND, How AI-Driven Welfare Systems Are Deepening Inequality and Poverty Across Europe, EUROPEAN AI FUND (Dec. 10, 2025), <https://europeanaifund.org/newspublications/how-ai-driven-welfare-systems-are-deepening-inequality-and-poverty-across-europe/>

³² Darrell M. West, How AI Will Transform the 2024 Elections, BROOKINGS INST. (May 3, 2023), <https://www.brookings.edu/articles/how-ai-will-transform-the-2024-elections/>

³³ 881 N.W.2d 749 (Wis. 2016)

³⁴ Significance of AI on National Voters' Day: Strengthening Democracy Through Innovation, INDIA AI (Jan. 23, 2025), <https://indiaai.gov.in/article/significance-of-ai-on-national-voters-day-strengthening-democracy-through-innovation>

norm. A locality marked as high-risk gets extra police, which leads to more stops, arrests, and input of data. This larger data set supports the model's prediction in the next cycle and pushes deeper the targeted neighborhood's risk profile. The algorithmic predictions over a period of time pretend to be objective when in reality they are just the amplified copies of historical discrimination. The latest reports from Amnesty International disclose that around 73% of police forces in the UK use predictive policing technology with very few human rights protections³⁵. These methods are not very clear, so it is hard for the affected people or the civil society to notice the bias and to challenge the decisions.

B. Welfare Algorithms - The Automation of Exclusion:

The government welfare systems are becoming more and more dependent on algorithms that are meant to detect fraud, assess eligibility, and allocate benefits. The reasoning behind this is similar to that for predictive policing spotting the data patterns and then making faster and more consistent decisions. As a result, in practice, welfare algorithms have turned into the means for discriminatory exclusion of the needy.

The Netherlands had a scandal that garnered much media attention when the tax department's algorithm-based system for processing childcare benefits applications considered applicants with other than Dutch nationality as "higher risk" for fraud³⁶. Families that were genuinely eligible and numbered in thousands were automatically subjected by the algorithm to further checks, rejections, and debt collection. The investigations exposed that the system had consistently mistreated individuals regarding their ethnicity and national origin which was against the Dutch equality laws. The same discrimination surfaced all over Europe.

Sweden's Social Insurance Agency used a fraud-predicting algorithm that primarily identified women, immigrants, and people with foreign-born parents, low-income earners, and those without higher education as potential fraudsters. Denmark's welfare agencies deployed algorithms that considered "unusual" living arrangements—like multi-occupancy homes, intergenerational households, and "foreign affiliations" as fraud risk indicators, hence effectively marking socially marginalized groups for monitoring through the use of social scoring mechanisms³⁷.

In Serbia, the automation of a World Bank-funded project utilized algorithms to identify the persons entitled to social assistance. The system was based on incorrect and incomplete information taken from government files, which led to unintentional disqualifications. Underprivileged groups like the Roma and the disabled were denied support that they were receiving before. These situations are an example of an important factor in determining the use of algorithms in welfare: they are not just processing neutral data, but also mirror and carry out the implicit policy choices concerning the trustworthiness of data, the "normality" of living conditions, and the degree of scepticism towards the claims. With the automating of decision-making, these biases get submerged in the mathematical models and the coding, thus concealing their source and making them harder to challenge.

C. Election Technology and Voter Profiling - Precision Targeting and Democratic Manipulation:

Election technology can be seen as a new frontier in the realm of algorithmic governance, and it has a massive impact on democratic processes and voters' rights. For instance, the Indian general elections of 2024 are a landmark in terms of AI usage in the electoral process. With the help of advanced AI analytics and massive datasets, political parties

³⁵ AMNESTY INT'L UK, Automated Racism: How Almost Three-Quarters of UK Police Forces Are Using Technology to Try to Predict Crime (2025), <https://www.amnesty.org.uk/predictive-policing>.

³⁶ Dr. Deborshi Barat, A Primer on Data Regulation and AI Development in India, NALANDA L. SCH. (Apr. 9, 2025), <https://forum.nls.ac.in/jilt-blog-post/a-primer-on-data-regulation-and-ai-development-in-india/>.

³⁷ LEXIS NEXIS, Data Protection and IP in India, L. ASIA (June 18, 2025), <https://law.asia/data-protection-ip-india-dpdpa-vs-gdpr/>

were able to create very detailed psychometric voter profiles and run micro-targeted messaging campaigns. The BJP, for instance, made use of the Saral App, which pooled together voter data (i.e. caste and religion) and applied algorithmic analysis to segregate the electorate, even using variables like electricity bills to come up with an estimate of socioeconomic status. This strategy made it possible to have a highly personalized political outreach in which the various voter segments were given completely different campaign messages that were not just based on their algorithmically inferred preferences and vulnerabilities but were also tailored to them³⁸.

While targeted outreach is one of the ways that can help engage voters, it can, at the same time, trigger the manipulation of democracy. Micro-targeting hides the information voters are getting; while one part of the electorate is hearing one story from a candidate, the other one is receiving the opposite one, so, to a certain extent, that isolation of public opinion is hindering the democratic process of deliberation³⁹. Besides, the 2024 elections in India were marked by the deployment of deep-fakes and AI-generated content, such as inauthentic video messages attributed to dead political leaders and Bollywood stars. These new technologies are eroding the base of democratic voting: the power to tell the difference between real and fake political communication is being gradually lost by the voters⁴⁰.

The problem is broader than mere trickery; it goes to political power's structural imbalance caused by technology. Politicians with better data and technology can move

easily and have more unblocked access to voters, thus, persuading them more. This means that the voters are no longer a homogeneous group in which ideas compete but a market where the one with better data and smarter algorithms will win⁴¹. Also through the use of commercial data brokers and inferred psychological profiles for targeting voters, the issue of voter privacy and freedom is brought to the fore. When the campaigns spot the people who are most receptive to certain appeals and then use very specific messages to take advantage of those weaknesses, they are, in fact, doing the opposite of giving the voters power and making them choose with full knowledge⁴².

III. HOW ALGORITHMS UNDERMINE DEMOCRATIC VALUES

A. The Transparency Crisis:

Systems for making decisions based on algorithms are typically not easy to understand. In the case of machine learning models, especially deep learning systems, there is a complete lack of transparency. They are likened to "black boxes," and their internal reasoning is still mathematically incomprehensible even to the people who built them. On the other hand, rule-based systems, while they can be theoretically more visible, are often kept as trade secrets and are patented. Even if the source code is made public, algorithmic systems usually rely on huge datasets whose composition and quality are not disclosed⁴³. The resultant lack of transparency poses a major governance problem: in democracies founded on the rule of law, both citizens and their elected representatives have the right to know how the government uses power. Administrative law insists that every decision must be reasoned,

³⁸ Algorithmic Accountability and Ethical Oversight: Legal Framework and Implementation Challenges, INT'L J. SCI. RESEARCH ARCHIVE 1 (2024), <https://ijsra.net/sites/default/files/IJSRA-2024-0722.pdf>.

³⁹ Transparency and Accountability in AI Systems, FRONTIERS HUM. DYNAMICS (July 2, 2024), <https://www.frontiersin.org/journals/human-dynamics/articles/10.3389/fhumd.2024.1421273/full>.

⁴⁰ Constitutional Democracy in the Age of Algorithms: The Implications of Digital Private Powers on the Rule of Law in Times of Pandemics, MEDIALAWS.EU (Nov. 10, 2020), <https://www.medialaws.eu/constitutional-democracy-in-the-age-of-algorithms-the-implications-of-digital-private-powers-on-the-rule-of-law-in-times-of-pandemics/>.

⁴¹ Consumer Online Privacy Rights Act: New Federal Privacy Bill Would Require Audits of Algorithms, DAVIS WRIGHT TREMAINE (June 30, 2020), <https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2020/01/consumer-online-privacy-rights-act>.

⁴² Niamh Kinchin, "Voiceless": The Procedural Gap in Algorithmic Justice, 32 INT'L J.L. & INFO. TECH. 79 (2024), <https://academic.oup.com/ijlit/article/doi/10.1093/ijlit/eaee024/7877312>

⁴³ Invisible Hand of Code: Reimagining Constitutionalism in the Age of Algorithms, NLIU L. REV. (Jan. 26, 2025), <https://nliulawreview.nliu.ac.in/blog/invisible-hand-of-code-reimagining-constitutionalism-in-the-age-of-algorithms/>.

that the officials must explain their choices, and that the affected parties must have the opportunity to express their views. The use of algorithms in governance contradicts these principles⁴⁴.

Predictive policing rarely reveals algorithms' inputs, training methods, and validation procedures, even to impacted parties and courts. Welfare algorithms are usually protected by vendor confidentiality claims, which restrict public scrutiny to a very limited extent. Election technology platforms use proprietary algorithms for content moderation and advertising delivery, rendering it impossible for either voters or election authorities to determine whether the information environment has been altered in any way⁴⁵. This inherent lack of transparency benefits both technology vendors and deploying agencies, as it protects their intellectual property and allows them to escape accountability for biased outcomes. However, it undermines the very core of democratic legitimacy. The public cannot agree with, oppose or change systems that are totally opaque to them⁴⁶.

B. The Accountability Fragmentation Problem:

The decision-making made by algorithms scatters accountability among different players like government, tech, and data players plus the developers within each organization. The theory of traditional administrative law is that an official or agency is solely accountable for a decision. The court looks into that official's reasoning and the justification presented. However, when a decision is taken through a complex interaction of social technology with the input of various organizations like algorithmic development, data collection, system integration, and

deployment, the issue of accountability becomes pretty complicated.

For instance, if a police predictive system gives discriminatory results, can we put the blame on the police department, the technology vendor, or the data scientists who trained the model, or everyone involved? In case of a welfare algorithm rejecting a claim, can the blame be placed on the government agency, the software company that built the system, or the data provider? These are the questions that the legal systems have not yet answered with the spreading of responsibility. The European Union's AI Act is one of the steps trying to clear up this matter by placing obligations on "deployers" of high-risk systems, meaning the parties who are going to use algorithms in making important decisions. However, the issue of who is responsible for the design and training of algorithms still remains unclear. Besides, even if responsibility is assigned, the channels for holding parties accountable are not very strong. A study on procedural justice conducted in 2024 found that while the measures for the fairness of algorithms and the frameworks for regulation take care of justice in terms of distribution, they create a "procedural gap" by not ensuring the necessary voice and participation in the decision-making process. The residents who are impacted by algorithm-based decisions usually do not have any significant means to challenge those decisions.

C. Civil Liberties Erosion - From Discrimination to Surveillance to Autonomy:

On the whole, algorithmic governance is a device that, more than anything else, takes away civil liberties. In the first place, it allows for large-scale deliberate and unintentional discrimination. The list of human ways to discriminate has one main requirement that of being as unobtrusive as to be unnoticed, and for that reason, there might be some case to argue one could lose and not be that much aware. In that case, a single welfare functionary, who for some reason was supposed to be

⁴⁴ Lord Sales, AI and Public Law: Automated Decision-Making in Public Administration, U.K. SUPREME CT. (Nov. 5, 2025), https://supremecourt.uk/uploads/speech_lord_sales_051125_db5ebd7036.pdf.

⁴⁵ Algorithmic Transparency as a Fundamental, BRAZILIAN J.L. & TECH. INNOVATION (2024), <https://bjlti.com/revista/article/download/19/18>

⁴⁶ OPEN GOVERNMENT PARTNERSHIP, Digital Governance: Open Government Guide 2024 on Automated Decision-Making, Algorithms, and AI (2024), <https://www.opengovpartnership.org/wp-content/uploads/2023/08/Open-Gov-Guide-2024-ADM-Algorithms-and-AI.pdf>

overly strict, might get the label of being discriminatory and thus lose the job. Algorithmic bias is hard to track down, to be contested and to change since it affects the whole system, and it is going to be able to render the same effect across the thousands of decisions made without being literally present in each of them.

In the second place, algorithmic governance would prompt an unprecedented level of monitoring. Police that use computer algorithms to predict criminal acts draw up a list of suspects for intensive surveillance, in some cases without the suspects even knowing about it and without their consent. The initiatives of the police in the UK to incorporate the predictive technologies were accompanied by a complete lack of the processes for the individuals flagged to contest their inclusion or even to know. Welfare organizations monitor the citizens of the UK, who is living with whom, their incomes and their employments through the use of digitized processes. Political consultancy firms elaborate on the voters' psychological characteristics and thus they also get to know their fears, dreams, and weaknesses⁴⁷. Often, such control is not just by the government but also by private tech firms that have access to the data for their own reasons.

Thirdly, algorithmic systems endanger psychological independence and freedom of thought. The rational reasoning of voters is affected when they are micro-targeted with custom-made political messages aimed at their perceived psychological weaknesses. When people are categorized by algorithms as "high-risk" criminals or "probable fraudsters," they tend to adopt these labels and their actions get influenced by the system's predictions. Thus, a certain kind of technological determinism emerges where algorithmic forecasts turn into self-fulfilling prophecies. People lose access to job opportunities, credits, and even security not for their past actions but

due to the future actions an algorithm anticipates⁴⁸.

IV. REGULATORY LANDSCAPES AND PROPOSED SAFEGUARDS

A. The European AI Act – Transparency and Explanation Rights:

The AI Act (2024) of the European Union is, as of now, the most thorough regulatory approach to artificial intelligence. The Act distributes compliance based on risk, applying the strictest rules to "high-risk" systems, the likes of which include and are not limited to, muscles in law enforcement, biometric identification, and protecting critical infrastructure. The system backpackers that deploy the technology are required to go through a whole process involving transparency, conduct conformity assessments and even, human oversight⁴⁹. Article 86 of the AI Act is the case whereby the rights of the affected individuals are put forward through the right to know clear and meaningful explanations of the AI system's involvement in the decision-making process and the major factors of the decision made. This can be viewed as a huge leap towards transparency but still with significant restrictions of the right⁵⁰.

One of the major restrictions is that the right is activated only in situations where a person believes that there is an adverse impact on health, safety, or fundamental rights, thus putting the burden of reporting harm on the affected individuals. In addition, the right to explanation has no link with the right to contest—the person may be informed of the reasoning behind the algorithm's decision but may not have legal grounds for it to be overturned.

B. India's Emerging Legal Framework – DPDP Act and Beyond:

⁴⁸ Algorithmic Transparency as a Fundamental, BRAZILIAN J.L. & TECH. INNOVATION (2024), <https://bjlti.com/revista/article/download/19/18>.

⁴⁹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 September 2024 on Artificial Intelligence (AI Act), OJ L 2024/1689 (2024).

⁵⁰ European Commission, Recital 159 to Regulation (EU) 2024/1689 ("The right to obtain explanation should not be construed as implying a right to reversal of the decision taken."); see also Art. 86

India's Digital Personal Data Protection (DPDP) Act 2023 offers a primitive yet promising platform for confronting harms related to algorithms, even though it was primarily aimed at data privacy rather than extensive AI governance. The DPDP Act compels "Significant Data Fiduciaries"—companies with vast amounts of personal data to process to carry out Data Protection Impact Assessments (DPIA), make them public and subject to annual audits that include also evaluations of the algorithmic systems in place for data processing. The law stipulates that the algorithmic systems must not violate the rights of the data subjects and, therefore, imposes the principles of data minimization and purpose limitation. Still, the DPDP Act is different from the EU GDPR in some significant aspects: it does not acknowledge other legal grounds for processing personal data like the "legitimate interest" which could hamper AI progress but, on the other hand, provide a strong barrier against illicit profiling⁵¹.

In February 2025, the India AI Advisory Group unveiled an extensive report that recommended a dedicated regulatory framework for AI in India. The report suggests algorithmic accountability, transparency, and participation of the stakeholders, as well as norms for different sectors, impact assessment for high-risk AI applications, and institutional setups for control. One of the particularly noteworthy proposals is to conduct obligatory algorithmic impact assessments prior to the launch of high-risk systems, and making the results available to the public for government use. Besides, the report urges the creation of an AI supervision body that would have the authority to certify, audit, and examine algorithmic systems, especially in the critical areas of criminal justice, welfare administration, and elections. These recommendations not only make it clear that regulatory support for algorithms will have to be specific, open, and

accountable but also that the regulation has to come forth.

On the other hand, challenges still exist. The data protection law in India has limited extraterritorial applicability that is only linked with the processing of data for the purpose of giving or selling goods or services in India, which could mean that foreign technology providers are free to handle data of Indian citizens without any constraints. Also, the existing situation where there are no specific rules protecting voter data and no requirement of transparency in the use of algorithms in the electoral process is a major shortcoming, especially considering the large-scale use of AI in Indian elections. The Digital India Act, which is being framed presently, can be used to fill these loopholes by establishing machine accountability and bringing in the related elections-specific safeguards.

C. The United States - Sectoral Regulation and Emerging Standards:

The legislative framework concerning artificial intelligence in the United States is missing a complete federal regulation, rather it is made of rules applicable to certain sectors together with gradually forming industry standards. The Algorithmic Accountability Act, which was initially proposed in 2019 and later revised in 2022, mandates that the systems making automated decisions that could have a major impact and are categorized as high-risk, must undergo impact assessments in the domains of credit, employment, and law enforcement, where these systems are used. The entities falling under this Act would have to provide a detailed explanation of the development of the system along with the training data, to check for accuracy and fairness, and to evaluate if the system produces negative effects with regards to the specified protected classes⁵². The Act would permit the Federal Trade Commission (FTC) to promulgate

⁵¹ PRS Legislative Research, The Digital Personal Data Protection Bill, 2023 (Bill No. 63 of 2023), https://prsindia.org/files/bills_acts/bills_parliament/2023/Digital%20Personal%20Data%20Protection%20Bill,%202023.pdf.

⁵² ActiveMind.legal, Article 86 – Right to Explanation of Individual Decision-Making AI Act (Nov. 12, 2024), <https://www.activemind.legal/legislation/ai-act/article-86/>.

enforcement rules by treating violations as unfair and deceptive trade practices. Although it has not yet been passed at the federal level, a number of states and local governments have started to implement akin initiatives. The Bias Audit Bill of New York City mandates that automated employment decision-making systems undergo bias audits prior to being set off. California Assembly Bill 13 suggests that algorithmic impact assessments should be carried out during the state agencies' procurement processes.

The American legal frameworks are all about flexibility and innovation, thus varying the regulatory intensity among different sectors. Nevertheless, this division results in some gaps. Bias auditing requirements prescribed by the federal government do not apply to predictive policing systems that most jurisdictions' municipal police departments are using. Moreover, state welfare systems are subject to different, and in some cases, no standards at all. In the absence of comprehensive regulations, the 'algorithmic harms' may just move to jurisdictions that are less strict in terms of supervision.

D. Proposed Integrated Safeguards – Toward Democratic Algorithmic Governance:

The democratic algorithmic governance has to rely on five safeguards:

1. Algorithmic Impact Assessments – Impact assessments that check for bias, exclusion, and civil liberties risks need to be done before the deployment of high-risk systems and also later in the life of the systems. These assessments should disclose the results and have them audited independently, especially in the public sector.

2. Transparency and Explanations – Authorities must with utmost clarity reveal the use of algorithms and provide affected individuals with comprehensible explanations and essential factors behind decisions. Moreover, the systems and data should be subjected to

audits with the exception of very few narrow cases.

3. Contestation and Redress – People should have the right to demand a review by a human as well as access to legal remedies. This includes the right to challenge the discriminatory systems and, where necessary, the shifting of the burden of proof to the side of the authorities in order to identify the hidden bias.

4. Independent Oversight Body – An authority that has a specific focus should take charge of the supervising of the algorithmic systems, responding to complaints, conducting audits on the deployments, and liaising with the different regulators that already exist but at the same time, keeping the institution independent.

5. Substantive Limits and Bans – Certain applications in which case predictive policing and completely automated decisions on the areas of sentencing, welfare, or voter eligibility fall should be subjected to strict limits, human review and transparency. Additionally, there should be explicit consent for political profiling and targeting.

CONCLUSION:

Algorithmic governance can help democracy only if the governments are transparent, rights-respecting, and accountable. Otherwise, the technology may kill the core values of constitutions. Predictive policing, social welfare sites, and voting devices all share in common the fact that AI based on historical data driven by efficiency, operating with the use of non-transparent models, and working under fragmented responsibility has led to discrimination, violation of civil rights, and making decisions that are not possible for people to understand, let alone contest effectively. This has to be dealt with by moving beyond just technical adjustments; it is requiring legal and institutional change, as seen in the developing models of the EU AI Act and India's data protection and AI frameworks. Thus, the democracies require the establishment of a

“digital constitutionalism” that regards the power of algorithms; whether it is exercised by the government or private sector as dependent on constitutional limitations. Among the main ideas of the digital constitutionalism are: all public decisions, including those taken by algorithms, must be logical, easy to understand, and subject to appeal; basic rights such as privacy, equality, and freedom of thought are fully applicable to AI systems; democratic legitimacy is dependent on transparency and real public involvement in determining the uses of AI which will have the highest impact; and the measures of accountability must be equal to the size and obscurity of the power of algorithms, with vulnerable groups receiving special support. Otherwise, governments may find themselves in a situation of technological authoritarianism, where citizens’ lives are quietly controlled by unaccountable algorithms rather than laws.