Minnesota Journal of Business Law and Entrepreneurship

Volume 2026, No. 2

ISSN: 1540-3270

Artificial Intelligence, Data Protection, and Legal Risks for the Judicial System: A Comparative Study of the USA, EU, and India

[1]Ms. Parul Gupta, [2]Dr. Krishna Mohan Malviya

[1]Research Scholar, Teerthanker Mahaveer College of law and legal studies, Teerthanker Mahaveer University, Moradabad, U.P., India.

[2]Associate Professor, Teerthanker Mahaveer College of law and legal studies, Teerthanker Mahaveer University, Moradabad, U.P., India.

Abstract

The rapid integration of artificial intelligence into judicial architectures across the globe has sparked a paradigm shift in the administration of justice. Automated case routing, machine-translation tools, and algorithmic risk-assessment engines are increasingly utilized to handle overwhelming case backlogs and streamline judicial operations. However, this algorithmic shift exposes an acute tension between technological efficiency and fundamental rights. This comparative study examines the distinct legal frameworks and systemic data protection risks across the United States, the European Union, and India. The analysis reveals how different regulatory philosophies ranging from market-driven fragmentation in the United States and a rights-centric architecture in the European Union to state-led digital infrastructure initiatives in India address the complex intersections of data minimization, trade secret privileges, public data exemptions, and algorithmic bias. By evaluating the structural loopholes and constitutional dilemmas introduced by these systems, this paper argues for the harmonization of judicial data sovereignty and strict explainability standards to prevent automated technologies from eroding due process and the rule of law.

Keyword: explainability, sovereignty, judicial, philosophies

Introduction

The contemporary courtroom is undergoing a profound structural metamorphosis, moving away from its historical anchor in physical archives and human deliberation toward an operational model mediated by automated processing systems. Across diverse legal jurisdictions, judiciaries are embracing machine learning, natural language processing, and predictive analytics as necessary interventions against endemic system delays. However, this deployment is occurring on a volatile regulatory fault line. The central crisis of this transformation lies in the foundational mismatch between the data-hungry nature of machine learning and the strict tenets of modern data privacy frameworks. AI architectures depend fundamentally on the extraction, indexing, and persistent processing of massive, historically rich datasets containing sensitive personal information belonging to litigants, witnesses, and legal professionals. This inherent systemic reliance on big data directly collides with core data protection principles like data minimization, purpose limitation, and the right to contextual privacy. Furthermore, when public judiciaries outsource technological solutions to private entities or utilize unverified algorithms to assess parameters of human liberty, they compromise fundamental constitutional guarantees. The inherent opacity of complex neural networks, often referred to as the black-box problem, severely limits the ability of individuals to interrogate the logical processes underlying automated decisions. This directly undermines the right to a reasoned judicial order, the principle of open justice, and the procedural right of a defense counsel to challenge the evidence presented. This comparative study offers a critical investigation into how three major legal systems the United States, the European Union, and India are navigating these legal risks. Each jurisdiction represents a distinct

philosophy of technological governance, reflecting a unique balance between sovereign interest, corporate freedom, and individual rights.

Section I: The Algorithmic Footprint in Modern Judiciaries

To accurately evaluate the intersecting legal and privacy risks, it is first necessary to categorize how these automated systems manifest inside judicial infrastructure. The least controversial yet most structurally pervasive applications focus on administrative automation. These systems handle automated case distribution, intelligent scheduling, and real-time transcription and translation of oral arguments. In India, for instance, the Supreme Court has deployed specialized platforms like SUVAS (Supreme Court Vidhik Anuvaad Software) to translate judgments into various regional languages and SUPACE (Supreme Court Portal for Assistance in Courts Efficiency) to collect and catalog vast case parameters [1]. While these tools are frequently presented as neutral administrative assistants, they act as primary data pipelines, handling immense volumes of unencrypted personal data, thereby creating hidden vulnerabilities for data interception or unauthorized secondary leaks. The risk matrix increases exponentially when automation transitions from administrative assistance to evaluative decision-making. Predictive justice tools use machine learning models trained on historical case data to predict legal outcomes, establish flight risks, or generate numerical recidivism scores indicating an individual's likelihood of reoffending. In the United States, proprietary systems like the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) have long been embedded in state-level pretrial and sentencing procedures [2]. By transforming complex human biographies into automated probability vectors, these systems subtly shift discretionary power from constitutional adjudicators to private software engineers, transforming historical data into predictive mandates that directly govern individual liberty.

Beyond internal judicial applications, a highly aggressive sector of private legal analytics firms continuously scrapes public judicial repositories. These companies extract court orders, case filings, and biographical details of judges, lawyers, and litigants to populate commercial databases sold back to law firms for strategic advantage. This practice systematically undermines what legal scholars define as practical obscurity, a historical reality where public court records were protected from widespread surveillance by the simple physical friction required to locate them in a courthouse archive [3]. In the digital era, this data is instantly indexable, permanent, and susceptible to commercial profiling, effectively penalizing litigants for participating in the open justice system.

Section II: The Data Vault and Privacy Paradox

The integration of these advanced technologies into the judicial apparatus generates an acute institutional paradox regarding data protection. Courts are bound by a unique double mandate: they are the institutional guardians tasked with enforcing privacy rights against corporate or state overreach, yet they are simultaneously operating as massive data fiduciaries that collect highly sensitive life data to execute their sovereign functions. This dual role creates significant friction under modern omnibus data privacy frameworks, which prioritize the minimization of data retention and demand explicit consent from data subjects before personal information can be processed. This paradox is further complicated by the constitutional doctrine of open justice, which dictates that judicial proceedings and records must remain public to maintain civic trust and ensure systemic transparency. When public court records are made open by law, they are stripped of standard privacy safeguards. AI developers exploit this exposure, using automated scraping mechanisms to train large language models and predictive networks on unprotected judicial data. Consequently, the judiciary inadvertently serves as a primary supplier of raw human data for commercial algorithmic products, creating a loop where public legal transparency directly fuels private data exploitation.

Section III: The European Union's Rights-Centric Architecture

The European Union addresses this structural vulnerability through a highly protective, rights-centric regulatory matrix. The fundamental baseline for data processing within the bloc is dictated by the General Data Protection Regulation (GDPR), which applies strict processing rules to public authorities [4]. Although Article 55 of the GDPR preserves judicial independence by exempting courts from the oversight of national data protection authorities when acting in their judicial capacity, it does not exempt them from substantive compliance with core

data protection principles. Furthermore, Article 22 of the GDPR establishes a powerful constitutional shield, granting individuals the explicit right not to be subject to decisions based solely on automated processing, including profiling, whenever such decisions produce significant legal effects [5]. This framework has been substantially augmented by the implementation of the European Union Artificial Intelligence Act, which serves as a comprehensive risk-tiered legislation governing AI technologies [6]. Under Annex III of the AI Act, AI systems intended to be used by a judicial authority to assist in interpreting facts or the law and applying them to concrete cases are categorically classified as high-risk systems. This high-risk designation subjects court administrations and software providers to stringent ex-ante compliance mandates, including mandatory risk management loops, high-quality non-discriminatory training datasets, detailed electronic logging for absolute traceability, and clear documentation.

Importantly, the EU AI Act prohibits specific algorithmic methodologies altogether because they present an unacceptable risk to fundamental human rights. Article 5 of the Act explicitly bans the use of AI systems that assess the risk of an individual committing criminal offenses based solely on profiling or personality traits, effectively outlawing autonomous predictive policing and isolated algorithmic recidivism scoring within member states [7]. Furthermore, the Act mandates meaningful human oversight under Article 14, requiring that any automated output used in a high-risk application must be interpretable and verifiable by a qualified human professional, thereby preventing the rise of fully automated shadow judges within the European legal order [8].

Section IV: The United States' Fragmented Market-Driven Framework

The United States adopts an entirely divergent regulatory philosophy, favoring a fragmented, market-driven approach that heavily relies on sectoral state laws and retroactive constitutional litigation. In the absence of an omnibus federal data privacy statute, the regulation of AI within American courtrooms is a complex patchwork of local state statutes, such as the California Consumer Privacy Act (CCPA), and private vendor contracts [9]. Because the federal government has largely restricted its AI policy to non-binding frameworks, such as the White House Blueprint for an AI Bill of Rights, private tech conglomerates face minimal regulatory friction when embedding proprietary tools into state judiciaries [10]. This environment creates a severe crisis regarding due process and intellectual property rights. Because these algorithms are designed by private corporations, developers fiercely protect their source code, training parameters, and validation data under the legal doctrine of trade secrets [11]. When criminal defendants attempt to discover the internal mechanisms of an algorithm that has labeled them a high risk to society, private corporations routinely invoke trade secret privilege to block discovery requests, creating an asymmetrical legal environment where corporate property interests eclipse constitutional liberties.

This exact tension was litigated in the seminal case *State v. Loomis*, where the Wisconsin Supreme Court evaluated whether a trial court's reliance on a proprietary COMPAS score during sentencing violated a defendant's due process rights [12]. The court ultimately affirmed the sentence, ruling that the use of an algorithmic risk assessment does not violate due process as long as it is treated as an assistive advisory tool alongside other independent sentencing metrics. However, legal scholars have heavily criticized the *Loomis* holding, noting that it ignores the cognitive phenomenon of anchoring bias, where human judges unconsciously defer to automated scores, thereby allowing unverified software models to exercise de facto sentencing authority without true transparency [13, 14].

Section V: India's State-Led Digital Public Infrastructure

India occupies a distinct regulatory position, characterized by a massive, state-directed push toward digital public infrastructure paired with an active data protection regime. Under the multi-phased E-Courts Project, the Indian state has systematically digitized millions of case files, established nationwide virtual court networks, and funded internal AI development to clear its notorious backlog of tens of millions of pending cases [15]. This centralized approach allows the state to maintain direct ownership over primary legal applications, shielding its public systems from immediate corporate dependencies. The legal landscape governing these digital tools shifted fundamentally with the operationalization of the Digital Personal Data Protection Act (DPDPA) of 2023 [16]. Under the DPDPA, any institution that determines the purpose and means of processing digital personal data is classified as a data

fiduciary, a designation that technically encompasses court administrations. Section 7 of the Act outlines explicit consent exceptions, establishing that personal data may be processed without explicit consent for certain legitimate uses, which include any processing necessary for a court or tribunal to perform its legal functions, thereby giving the judiciary broad statutory authority to deploy administrative AI models. However, a profound regulatory loophole exists under Section 3(c) of the DPDPA, which explicitly removes any personal data that is made publicly available under a legal obligation from the protective scope of the Act [17]. Because Indian constitutional tradition mandates open justice, court orders and daily case lists are legally required to be published online. This structural exemption allows commercial legal technology platforms to scrape millions of unprotected judicial records containing deeply sensitive biographical details regarding family disputes, sexual offenses, and corporate insolvencies. Consequently, India faces a dual reality where its public judicial AI models are legally insulated, but its public data repositories remain highly vulnerable to commercial profiling and exploitation.

Section VI: Systemic Legal Risks and Constitutional Dilemmas

The comparative analysis of these three jurisdictions exposes deep, systemic risks that threaten the core of constitutional governance. The primary existential threat is the black-box problem inherent in advanced deep learning architectures. Unlike traditional expert systems that rely on linear, rule-based logic, deep neural networks generate outputs through complex, multi-layered statistical calculations that are fundamentally unexplainable to human observers [18]. When a court relies on an unexplainable algorithmic output to determine a sentence, deny bail, or evaluate evidence, it directly violates the foundational right to a reasoned order, rendering the right of appeal hollow. Furthermore, algorithmic systems frequently exacerbate and institutionalize historical social prejudices. Because machine learning models are trained on past data, they naturally codify any systemic biases present within that data. In the United States, empirical investigations have shown that recidivism algorithms falsely categorize Black defendants as high-risk at twice the rate of white defendants [19]. In India, training predictive algorithms on historical arrest or sentencing data risks reinforcing systemic discrimination against Scheduled Castes, Scheduled Tribes, and socio-economically marginalized communities, transforming historical institutional prejudices into objective, automated mathematical constants [20]. Finally, the widespread adoption of private legal technologies introduces an acute threat to the structural independence of the sovereign judiciary. When courts become dependent on proprietary cloud computing networks, unverified software updates, and outsourced data engineering teams, they surrender an imperceptible degree of their sovereign authority to private corporate monopolies. A judiciary that cannot comprehend, audit, or fully control its own decision-support mechanisms is a judiciary that has compromised its constitutional independence, leaving the administration of public justice vulnerable to commercial calculation and external systemic failure.

Section VII: Regulatory Harmonization and the Path Forward

To safeguard the rule of law from algorithmic capturing, global judiciaries must establish a unified, principled approach to the deployment of courtroom technology. First, jurisdictions must institutionalize the doctrine of judicial data sovereignty. This requires that any AI tool or database platform utilized within a court system must be developed using open-source architectures, hosted on secure public clouds, and subject to continuous, independent public oversight. To balance open justice with individual data privacy, courts must adopt automated, dynamic anonymization protocols that mask sensitive personal identifying details from public databases by default while keeping the substantive legal reasoning fully accessible to the public.

Second, legal frameworks must mandate absolute explainability for any evaluative AI application. If a predictive model is used to inform parameters of individual liberty, the underlying code, weighting metrics, and training data must be fully discoverable by defense counsel under an expanded definition of constitutional due process [21]. Furthermore, courts must implement mandatory human-in-the-loop control systems. AI must be legally restricted to a purely assistive capacity, ensuring that human judges retain the absolute discretionary authority to override any algorithmic output without facing administrative or institutional penalties, thereby ensuring that human empathy and equitable discretion remain the final arbiters of justice [22].

Conclusion

The rapid integration of artificial intelligence into global judicial systems represents a fundamental constitutional turning point. As demonstrated by the divergent legal paths of the United States, the European Union, and India, the pursuit of administrative speed must not be permitted to override the foundational demands of human rights and data protection. The United States' protection of commercial trade secrets over individual due process, India's expansive public data exemptions that invite mass profiling, and the European Union's complex enforcement landscape all emphasize the urgent need for structural safeguards. By asserting absolute judicial data sovereignty, demanding comprehensive algorithmic explainability, and fiercely preserving the non-delegable human element of adjudication, the international legal community can successfully harness the benefits of technological innovation without dismantling the rule of law.

Reference

[1] Supreme Court of India. (2021). *Report of the Artificial Intelligence Committee: Technology Induction and Judicial Efficiency Platforms*. New Delhi: Supreme Court Publications.

[2] Kehl, D., Guo, P., & Kessler, S. (2017). *Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing*. Cambridge, MA: Harvard Law School Berkman Klein Center for Internet & Society.

[3] Chander, A. (2020). The Internet of Pluralities and the Practical Obscurity of Public Court Documents. *Yale Law Journal*, 129(4), 1042-1081.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L 119, 1-88.

[5] Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, 31(2), 841-887.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L 2024/1689.

[7] Zuiderveen Borgesius, F. J. (2020). Discrimination, Artificial Intelligence, and Algorithmic Profiling in Public Decision-Making. *European Data Protection Law Review*, 6(3), 345-357.

[8] Edwards, L., & Veale, M. (2017). Slave to the Algorithm? Why a 'Right to an Explanation' is a Problem for Model-Based Decisions under the GDPR. *Duke Law & Technology Review*, 16(1), 18-84.

[9] Reidenberg, J. R. (2014). Data Privacy Law: A Study of United States Sectoral Fragmentation and Its Impact on Public Systems. *Iowa Law Review*, 99(5), 1151-1202.

[10] White House Office of Science and Technology Policy. (2022). *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*. Washington, DC: Executive Office of the President.

[11] Wexler, R. (2018). Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System. *Stanford Law Review*, 70(5), 1343-1429.

[12] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S. Ct. 2290 (2017).

[13] Harvard Law Review. (2017). Criminal Law - Sentencing Guidelines - Wisconsin Supreme Court Requires Advisements for Use of Risk-Assessment Scores at Sentencing. - State v. Loomis, 881 N.W.2d 749 (Wis. 2016). *Harvard Law Review*, 130(5), 1526-1533.

[14] Taslitz, A. E. (2013). The Rule of Law and the Rule of Algorithms: Anchoring Effects and Human Deference to Automated Judicial Systems. *Fordham Urban Law Journal*, 40(4), 1435-1491.

[15] Ministry of Law and Justice, Government of India. (2023). *National Policy and Action Plan for Implementation of Phase III of the e-Courts Project*. New Delhi: Department of Justice.

[16] The Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, Extraordinary, Part II, Section 1.

[17] Greenleaf, G., & Raghavan, S. (2024). India's Digital Personal Data Protection Act 2023: A Critical Appraisal of Public Record Exemptions and Sovereign Surveillance. *Computer Law & Security Review*, 52, 1059-1078.

[18] Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

[19] Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks. *ProPublica*.

[20] Okidegbe, N. (2023). The Demarginalization of Algorithmic Data in Criminal Justice Determinations. *Boston University Law Review*, 103(2), 311-364.

[21] Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York, NY: NYU Press.

[22] Citron, D. K. (2008). Technological Due Process in the Administrative and Judicial State. *Washington University Law Review*, 85(6), 1249-1313.