International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

ARTIFICIAL INTELLIGENCE AND LAW: ISSUES OF PRIVACY, LIABILITY and REGULATION

Hitesh Lathar

UGC / NET Qualified, Department of Law

ABSTRACT

In the areas of governance, commerce, healthcare, criminal justice and now all consumer technology, the rollout of artificial intelligence ("AI") has surpassed the doctrinal categories upon which the law has traditionally depended to allocate rights, duties and remedies. This paper looks at three intertwined legal issues arising from the use of AI systems: the loss of informational privacy as a result of the pervasive collection of data and the prediction of behaviour; the question of how to allocate, apportion or locate civil and criminal liability within an autonomous, opaque and probabilistic technological process; and the difficulty of formulating regulatory instruments that can govern a general purpose technology without restricting innovation. With reference to various legal frameworks, including the General Data Protection Regulation, the Digital Personal Data Protection Act, 2023 (India), the European Union's Artificial Intelligence Act and common law principles of torts, alongside recent cases and decisions such as Mobley v. Workday, the Clearview AI litigation, the Cambridge Analytica enforcement action and the State v. Loomis case, this paper analyzes how existing laws are being adapted, sometimes awkwardly, to fit the world of AI and challenges the efficacy of the one-size-fits-all liability approach. The paper concludes that privacy, liability and regulation cannot be considered as separate boxes, but a reinforcing framework of algorithmic accountability – future law reform should consider these concepts as a whole.

KEYWORDS: Artificial Intelligence; Data Privacy; Algorithmic Liability; Tort Law; Data Protection Regulation; Automated Decision-Making; Artificial Intelligence Act

INTRODUCTION

AI is not a future or abstract concern of legal scholarship: it is a working part of the modern regulatory state and modern marketplace. From facial recognition in public areas to recommender systems that dictate what consumers see and purchase, from credit scoring to hiring and from text generation to image generation – including even legal documents – generative AI systems are present across various domains with minimal human intervention. All of these applications create legal issues at a nexus of well-established privacy, tort, contract, criminal procedure and constitutional law. The problem is that the central challenge is that AI systems especially algorithms based on machine learning don't easily fall into the conceptual language of law as it's evolved to distribute blame. While the traditional negligence doctrine requires the presence of an identifiable human actor with an identifiable conduct to be measured against a standard of reasonable care, AI systems are more likely to act as an intermediary whose decision logic is statistically based, continually updated and frequently unknowable even to those designing the algorithm. Personal information is traditionally thought of as being revealed or not revealed, while AI systems can infer sensitive information – health status, sexual orientation, political opinion – from seemingly benign data, blurring the line between what information is disclosed and what information may be inferred. However,

the traditional approach to regulatory design depends on the ability to narrow down a technology to the point that it can be comprehensively regulated through a sector-specific approach, which is problematic in the case of AI because it is a general-purpose technology and requires a horizontal, risk-based regulatory approach (Kerrigan, 2022).

For comparative AI law, the paper is structured around three thematic clusters which feature throughout the paper: privacy and data protection; civil and criminal liability; and regulatory design. Representative judicial decisions, statutory provisions and scholarly comments are examined in each cluster. The paper is divided into five substantive parts.

In the first part, the authors analyse how AI affects the right to privacy and how courts and legislatures have responded to this challenge. In Part 1, the authors explore how AI is affecting the right to privacy and how courts and legislatures are reacting to it. The survey in Part II reviews frameworks for data protection which have been adapted, or newly introduced, to cover data processing using AI. Part III discusses the developing principle of civil and criminal accountability for the damage caused by AI. Algorithmic decision-making, due process and discrimination are discussed in Part IV, focused on the application of AI in the fields of criminal justice and employment. Part V conducts a comparative overview of regulatory approaches, concluding with a consideration of the European Union's AI Act, marking the first extensive horizontal regulatory framework of its kind. The paper ends with a comprehensive overview of the current state of the law and proposals for reform (Calo, 2017).

ARTIFICIAL INTELLIGENCE AND THE RIGHT TO PRIVACY

The constitutional fabric that AI is poised to undermine is based on the right to privacy. Doctrines of informational self-determination, reasonable expectation and control over disclosure have long provided protection for privacy. Each of these conditions is being overturned by AI systems. There are many instances where private and state actors can build detailed portraits of individuals without their consent, even when the data was not originally designed for identification or prediction. Large-scale data scraping, biometric identification and inferential profiling are all technologies that enable private or state actors to develop detailed descriptions of individuals without their awareness or meaningful consent and sometimes without the data ever having been used for identification or prediction.

The Erosion of Consent-Based Privacy

Traditionally, the main legal means proposed to give people "control" over their personal data is through consent. AI-powered data collection threatens this mechanism in two ways. First, because the scale and opacity of data harvesting, for example by mass-scraping of publicly posted photographs for the creation of facial recognition databases make meaningful, informed consent virtually unattainable. Second, machine learning models can also uncover new classes of sensitive personal data from information that may have been shared for a completely different objective, regulators have called "function creep. The consequence of this is that the consent, even if given, no longer serves its purpose of allowing people to manage the downstream uses of their data (Nissenbaum, 2014).

Biometric Data as a Site of Heightened Risk

Facial geometry, fingerprints, iris scans and voiceprints are among the types of biometric identifiers that have come to represent a uniquely polarized form of personal data, being

unchangeable, unique and vulnerable to extraction by AI from common images and videos. Cases under specific laws concerning biometric information have resulted in some of the most significant AI privacy case law to date, both in terms of the amount of liability and the shortcomings of a reactive, litigation-based approach to privacy protection.

Case: Illinois v. Clearview AI, Inc. and the related multi-district litigation, the facial recognition firm obtained billions of pictures from social media without the user consent, creating a searchable biometric identification database. As a result of the Illinois Attorney General's action under the Biometric Information Privacy Act, the settlement includes a nationwide injunction preventing Clearview from selling its database to private companies, in addition to data protection authorities in the United Kingdom, France, Italy and Australia issuing fines and enforcement orders. The litigation clarified the issue of consent to the processing of biometric data by the mere fact of its being scraped from publicly visible photos and the fact that territorial data-protection laws could apply if the data processor operates in that jurisdiction.

Rogers v. BNSF Railway Co. presents an example of a jury awarding approximately USD 228 million in statutory damages for approximately 45,600 reckless or intentional violations of the Biometric Information Privacy Act (BIPA) by the defendant railway company in connection with the use of a biometric time-clock system operated under the auspices of a third party vendor. The judgment serves as a reminder of the potential for harm that biometric AI technologies can create, even in seemingly mundane, non-consumer use cases in the workplace and of the fact that an employer remains liable when outsourcing biometric processing to a vendor.

Article: Illinois Biometric Information Privacy Act, 740 ILCS 14/1 et seq. (2008), especially section 15, which mandates informed written consent before collecting biometric identifiers and provides a private right of action for statutory damages. The Biometric Information Privacy Act (740 ILCS 14/20) prescribes liquidated and statutory damages for negligent and reckless or intentional violations of the Act and sec. 15(b) contains a "duty to obtain informed consent before collection.

Privacy as a Constitutional Right and Its Application to AI

Where privacy is treated as a constitutional right, the law on automated data processing has started to be interpreted as such. As the Indian Supreme Court has deemed privacy to be a fundamental right, it has also laid a precedent for the upcoming development of privacy laws governing AI use of data in India, such as the Digital Personal Data Protection Act, 2023.

Case: This case was heard by a nine-judge bench of the Supreme Court of India which unanimously ruled that the right to privacy is a basic right guaranteed by the Constitution of India, intrinsic to the right to life and personal freedom of the person and to the freedoms of expression, movement and personal freedom guaranteed by Part III of the Constitution. Since that time, the judgment has drawn upon informational privacy as an independent part of the constitutional right and it has been invoked to challenge the constitutionality of state surveillance, biometric identification systems and increasingly state and private sector AI-based data processing systems.

Article: Article 21 of the Indian Constitution which guarantees right to life and personal liberty in conjunction with Article 19(1)(a) and the doctrine of substantive due process as laid out in the Puttaswamy case and Article 8 of the ECHR which protects the right to respect for private and family life. All of this shows the extent to which AI has added to the pressure on current privacy law, rather than generating a completely new branch of privacy law, but instead has caused courts and legislatures to issue new interpretive and statutory answers, which will be discussed more thoroughly in Part II below.

DATA PROTECTION FRAMEWORKS AND AI: FROM THE GDPR TO THE DPDP ACT

Part I showed that AI challenges the doctrine of privacy; this Part focuses on the legal frameworks that have been built – or adapted – to manage AI-based data processing in the statutory sphere. The current state of data protection law is that it serves as the main tool by which the majority of jurisdictions control the data-related actions of AI, due to the lack of a comprehensive piece of legislation on AI in nearly all parts of the world except the European Union.

The General Data Protection Regulation as a Templat

The principles of lawfulness, purpose limitation, minimisation of data, accuracy and accountability are authorized by the European Union's General Data Protection Regulation and have since been adopted as the model for data protection laws globally. The Regulation's provisions on automated decision-making, including profiling, are of particular relevance in relation to the work of AI, providing data subjects with a qualified right not to be subject to a decision based on automated processing, which produces a legal or similarly significant effect, with the exception of the specific exceptions and safeguards, including the right to obtain a human intervention and the right to contest the decision

Case: With respect to whether facial recognition trained with data obtained from scraped images is covered by the territorial scope and the material scope of the GDPR, case law of the UK Information Commissioner's Office, the French Commission Nationale de l'Informatique et des Libertés and the Italian Garante per la Protezione dei Dati Personali suggest that the processing is under the Regulation's scope even if the processing entity is not established in the EU, but where the processing is related to the monitoring of the behaviour of individuals in the EU.

Article: (EU) 2016/679 (General Data Protection Regulation), Article 5 (principles relating to processing), Article 9 (processing of special categories of personal data, including biometric data), Article 22 (automated individual decision-making, including profiling), Article 3 (territorial scope).

India's Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 is India's first comprehensive general data protection law and extends to processing of digital personal data in India or related to providing goods or services in India to data principals in India, including for AI training and deployment, thus having a direct jurisdictional connection with India. The Act follows a "consent and notice" framework, adds a "certain legitimate uses," places duties on data fiduciaries concerning accuracy and security measures and provides for notification to major data

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 7.2 Website: https://ijarmt.com ISSN No.: 3048-9458

fiduciaries that are required to implement enhanced obligations, which will presumably cover large-scale AI developers using data (Greenleaf, 2023).

Case: The Puttaswamy framework of proportionality and legitimate state aim has been applied to the assessment of the validity of automated data-processing schemes, including automated identification systems such as Aadhaar, by Indian courts and this interpretive lens will be likely followed by the judiciary as cases relating to AI are brought before it

Article: Article 257 of the GDPR, along with sections 4–9 of the Digital Personal Data Protection Act, 2023 (India) (which outline obligations of data fiduciaries and grounds for processing) and section 8(1) of the Act (accuracy and completeness of personal data) and section 33 of the Act (financial penalties for non-compliance, up to INR 250 crore for failure to implement reasonable security safeguards).

A Comparative Patchwork: CCPA, LGPD and the Multi-Jurisdictional Problem

The U.S. doesn't have a comprehensive federal privacy law and of the state laws that do exist, the California Consumer Privacy Act, which was significantly expanded by the California Privacy Rights Act, is the most significant in the context of AI data processing, including provisions for consumers' rights to know, delete and opt-out of the sale or sharing of their personal information and subsequent rulemaking of rights relating to automated decision-making technology. Compliant with similar laws in other jurisdictions, such as Brazil's Lei Geral de Proteção de Dados, these laws offer similar protection, but the resulting patchwork creates multi-jurisdictional compliance obligations for AI developers operating across borders (Katshir, 2020). It is noteworthy, however, that in 2025 the California Privacy Protection Agency will finalize regulations under the California Consumer Privacy Act that apply to automated decision-making in the context of other significant choices affecting individuals, including those in the employment context and that also make the businesses using such technology liable, not just for the product or service, but also for the technology itself, even if outsourced to a third party vendor. CCPA (California Consumer Privacy Act of 2018), Cal. Civ. Compare California Privacy Rights Act of 2020, law No. 1798.100 and the 2025 California Privacy Protection Agency's regulations on Automated Decision-Making Technology; Lei Geral de Proteção de Dados, law No. 13,709/2018 (Brazil), Article 20 (right to review of automated decisions). While there are distinct differences in the intensity of the regulations and the extent to which various jurisdictions draw the line between automated decision making that can be made without meaningful human participation and automated decision making that requires meaningful human participation, there are common themes emerging from the comparative surveys in this Part, in particular in relation to the regulatory grammar of the four principles: lawful basis, purpose limitation, data-subject rights and accountability.

CIVIL AND CRIMINAL LIABILITY FOR AI-CAUSED HARM

The need for a more comprehensive view of liability in AI cases has never been more evident than it is now. In the negligent model of tort law, some human actor is assumed who can be assessed against an objective standard of care and who can be shown to have contributed to harm via a reasonably foreseeable chain of events. Each element of the framework is made challenging by the addition of AI. The ‘actor' can be a statistical model whose results are

probabilistic, not deterministic; the behaviour can be of the developer, the deployer, or the end user; and causation can be hard to prove, even for the model's creators if the model's decision-making process is not fully interpretable.

Product Liability and Autonomous System

In relation to the first question of whether a defective or negligently designed AI system is a defect, courts have tended to adopt the existing product liability doctrine, reasoning that a defective or negligently designed AI system is similar to a defective mechanical component and have struggled with the more difficult issue of what the standard of "defectiveness" should be compared to in a system with an autonomous entity, it should be compared to a reasonable human driver, a reasonable engineer, or the actual performance of comparable autonomous systems, for example.

Case: Litigation stemming from crashes involving vehicles operating in partially automatic driving modes has pushed the boundaries of product liability, design-defect and failure to warn doctrines, with courts taking a fact-specific and incremental approach to autonomous-vehicle liability – not necessarily into a new liability paradigm, as the courts' stance in a widely reported ruling of 2025 suggests the manufacturer's marketing representations on system capability and not the technical performance of the software, should dictate the analysis of liability.

Article: See also the proposed Directive (EU) 2024/2853 on liabilities for defective products which explicitly expands the definition of "product" to include software and AI systems and places a lighter burden on the claimant to establish the software's defectiveness and causation where such proof is "technically complex.

Liability for Generative and Autonomous Software Outputs

The liability problem is different with generative AI systems because their results are not products; they are informational content (text, images, or code) that is likely not directly authored by the human who is using the specific content-generating tool and may be harmful (false, defamatory, or otherwise), or cause harm. This has led to the first round of defamation and related tort lawsuits against the AI developers themselves.

Case: A radio host in Georgia has brought what commentators say is the first defamation case against an AI developer in 2023 when, upon being asked by a journalist, a generative chatbot made up a bogus legal claim of embezzlement from a non-profit organisation against him. The case made the novel point that a developer may be liable in defamation for publishing or otherwise disseminating a false statement of fact that was created without human input, but rather by the developer's model and has been a subject of later discussion on the application of traditional publisher/distributor liability principles to generative AI.

Article: Artificial Intelligence Liability Directive (proposed), COM (2022) 496 final, article: Restatement (Second) of Torts §§ 558-559 (elements of defamation) and § 581 (distributor liability).

Vicarious and Interception-Based Liability for Deployers

Another type of litigation, growing in importance, is against the company that is using the AI model and involves provisions in wiretapping and electronic-communications statutes that were enacted decades ago before the advent of AI.

Case: In Jones v. Peloton Interactive, Inc., Plaintiffs claimed the Defendant was in violation of the California Invasion of Privacy Act because the Defendant had installed an AI-powered third party chat on its website and used that tool to intercept and record users' communications without their consent, which the court did not dismiss. A federal judge in that same case in Taylor v. Converse Now Technologies allowed a potential class action to move forward against a company offering an AI voice assistant for restaurant phone orders and asked whether an AI vendor was a "liable 'third-party' interceptor" whose data could be used for both the customer's order and the vendor's own commercial goals, including model improvement

Article: They are prohibiting the wife from entering California. They are blocking the wife from getting into California. Prohibiting the wiretapping or unauthorized interception of communications (Penal Code § 631) as it applies to AI chat and voice assistants built into commercial websites and call-handling systems.

The liability framework surveyed in this Part can be described as one of doctrinal extension and not doctrinal invention: courts have been rather reluctant to establish new "AI torts", preferring to extend existing torts such as product liability, defamation and statutory interception; and legislators, especially in the European Union, have taken steps to create new instruments for liability, which shift the burden of proof to reflect the opacity of AI.

ALGORITHMIC DECISION-MAKING, DUE PROCESS and DISCRIMINATION

In cases where AI systems are used to influence or inform decisions that have a significant impact on individuals, such as sentencing, parole, hiring, credit and benefits eligibility, the issue becomes one of procedural justice and equal treatment, rather than privacy and compensation. This Part reviews the most prominent legal scholarship on algorithmic due process and discrimination, focusing on the issue of due process in the criminal justice and employment settings.

Algorithmic Risk Assessment in Criminal Sentencing

The number of criminal sentences made by judges using proprietary risk assessment algorithms has led to the most sustained judicial interaction with the due process concerns of opaque, "black-box" AI decision-making.

Case: The defendant in State v. Loomis argued that the circuit court was wrong to rely on the COMPAS risk-assessment score, which was a proprietary algorithm whose methods were not made available to the defense, because he could not challenge the scientific soundness of the score. When used in a sentencing proceeding, a court's consideration of a COMPAS assessment is not a denial of due process as long as the assessment is not the only or most important basis for a sentence and the sentencing court is given a notice that conveys specific warnings regarding the limitations of the tool, such as cautions in the area of group-based statistical validation and problems with disparate racial impact. It has been decried by many scholars as allowing the continued use of a tool that is proprietary and a trade secret of the algorithm's creators, so that it will not be subjected to the proper adversarial testing required in criminal law and is the top precedent in American criminal law for algorithmic due process.

Article: The articles of the Constitution of the United States of America. Cautionary information in a sentencing judgment about the proprietary nature of a risk-assessment tool, its individual-level accuracy and studies indicating that the tool may have a disparate impact on

minority offenders, but not the algorithm itself, is required pursuant to XIV, § 1 (due process clause).

Algorithmic Discrimination in Employment

A novel category of discrimination litigation, centered on the question of whether pre-existing civil rights and employment laws, some of which predated the dawn of computerised hiring, apply to software vendors that do not actually hire the applicant, has emerged.

Case: In the case of Mobley v. Workday, Inc., plaintiff claimed that the defendant's (the company behind the AI applicant screening tools) AI-powered tools discriminated against applicants based on race, age and disability. The court rejected the plaintiff's Title VII, Age Discrimination in Employment Act, Americans with Disabilities Act and intentional-discrimination theories brought against Workday as an agent of the employers, but allowed the plaintiff to proceed with claims against Workday on the theory that it was an "employment agency" under Title VII and also allowed claims to proceed under California's Fair Employment and Housing Act (FEHA) and granted plaintiff the opportunity to amend claims against Workday for intentional discrimination under Title VII, the ADEA and 42 U.S.C. § 1981. The ruling is noteworthy for affirming, in a reported federal ruling for the first time, a plausible direct liability theory for an AI vendor whose software is used by many downstream employers to make consequential employment decisions.

Article: Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e-2 (prohibiting discrimination by employers and, as interpreted here, by entities that act as employment agencies); Age Discrimination in Employment Act, 29 U.S.C. § 623; Americans with Disabilities Act, 42 U.S.C. § 12112; California Fair Employment and Housing Act, Cal. Gov't Code § 12940.

Prohibited and High-Risk AI Practices in Comparative Regulation

The legislative reactions to algorithmic discrimination and due process issues have now turned upstream from litigation, banning or substantially restricting certain types of AI usage before they can even become problematic, rather than simply providing remedies after the fact.

Case: The principles contained in the White House Office of Science and Technology Policy's case regulatory guidance, though not mandatory, have also been cited by state attorneys general and litigants in subsequent AI discrimination disputes, such as the California Privacy Protection Agency's regulations regarding automated decision-making technology, which are discussed in Part II.

Article: White House Office of Science and Technology Policy, Blueprint for an AI Bill of Rights (2022), which sets forth five principles: safe and effective systems, algorithmic discrimination protections, data privacy, notice and explanation and human alternatives, consideration and fallback; Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 5 (Prohibited AI Practices), Article 6 read with Annex III (Classification of high-risk AI systems, including AI systems used in the field of employment and in law enforcement and administration of justice).

Many of the cases and instruments covered in this Part feature the same structural issues: algorithmic opacity, whether through trade secrecy as in Loomis, or through vendor architecture, as in Mobley, poses a threat to the adversarial and participatory core of due

process and anti-discrimination law. Regulatory responses discussed in Part V are attempts to deal with this concern on a systemic basis as opposed to on a case-by-case basis.

COMPARATIVE REGULATORY APPROACHES TO ARTIFICIAL INTELLIGENCE

As illustrated in the preceding Parts, the courts and regulators, so far, have applied existing doctrine to privacy, data protection, tort and anti-discrimination law basis-by-basis, at least in part, to accommodate AI. This final Part analyzes new generation of AI specific regulation instruments which seek to take a more systemic, ex ante approach and places these instruments within a wider typology of regulatory strategies, comparative to the others. It is the first horizontal law of its kind in Europe and aims to tackle a wide range of AI applications, is risk-based, which means that certain uses are banned outright, while others require conformity assessment, documentation and oversight by humans and transparency requirements are relaxed in the case of low-risk systems, such as chatbots and deepfake generators. The Act extends beyond the territories of the Union, with elements of the "Brussels effect," which is the model used in the GDPR, meaning that AI developers outside the Union will likely have to comply with its requirements when placing systems on the Union market or using outputs in the Union (Zuiderveen Borgesius, 2021).

Until now, the Indian government has not enacted any specific AI laws, relying on the Digital Personal Data Protection Act, 2023, to govern data obligations; the Information Technology Act, 2000, for intermediary obligations and cybersecurity; and, non-binding guidelines issued by the Ministry of Electronics and Information Technology to guide AI developers and platforms in the country, while keeping an eye on countries such as the European Union who have already enacted the EU AI Act.The Indian government has so far avoided binding horizontal laws on AI, instead opting for a national policy stance that aims to foster innovation and adoption, while watching developments in other jurisdictions, including the EU AI Act and taking guidance from it where appropriate.

Case:

- The European Commission and national market-surveillance bodies under the Artificial Intelligence Act have issued regulatory guidance and established early compliance priorities that explicitly reference the harms that have already been litigated in the Clearview AI and State v. Loomis cases, which will result in judicially identified harms being transformed into a codified, prospective compliance obligation.
- While India does not have legislation specific to AI, courts have used the proportionality test developed in Puttaswamy in the context of AI to evaluate state use of automated and biometric identification systems, as was done in challenges to the constitutional validity of the Aadhaar biometric identification scheme; this test provides an interpretive framework that may guide future cases in which state use of AI is challenged before India passes legislation specifically designed for AI.
- The Federal Trade Commission's settlement with Facebook, Inc. over the Cambridge Analytica scandal, in which the personal data of users harvested through a third-party quiz app was used to make psychographic profiles for political micro-targeting without their consent, was the

- biggest privacy enforcement action by any U.S. regulator against a tech firm and imposed the largest civil penalty ever.

Article:

- Harmonised rules on artificial intelligence (Artificial Intelligence Act) (Articles 5, 6 and Annex III, prohibiting the use of real-time, remote biometric identification in publicly accessible spaces for law enforcement purposes, with narrow exceptions and of social-scoring systems and Article 9, obligations on providers of high-risk AI systems regarding risk-management systems).
- Federal Trade Commission Act, 15 U.S.C. § 45 (banning unfair or deceptive acts or practices), as applied in the 2019 FTC-Facebook consent order and Executive Order 14110 of October 30, 2023, on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence, which calls on federal agencies to provide AI risk-management guidance on a sector-by-sector basis instead of comprehensive legislation.
- The Information Technology Act, 2000, sections 43A (compensation for failure to protect sensitive personal data) and 72A (punishment for disclosure of information in contravention of a lawful contract); Advisory on Due Diligence by AI Platforms and Intermediaries (2024), issued by Ministry of Electronics and Information Technology; National Strategy for Artificial Intelligence #AIforAll (2018), issued by NITI Aayog.

CONCLUSION

In this paper, I have looked at the legal implications of AI in three interconnected areas (privacy, liability, regulation) and posited that no one area can be considered without the other. Erosion of consent-based privacy, as outlined in Part I, establishes the informational environment in which algorithmic decision-making, explored in Part IV, is possible and consequential. The doctrinal strain identified in Part III is based on just such processes of AI systems and the collection of vast inferential datasets, described in Part I and Part II. In all the jurisdictions studied, the regulatory measures in Part V have evolved from privacy or liability claims that have been adjudicated in court to more formalized rules.The regulatory measures in Part V are in all jurisdictions studied responses to harms identified through judicial rulings, which were first to be recognized as privacy or liability disputes and only then formalized into rules.

Three conclusions follow. In the interim, courts from a variety of jurisdictions have consistently rejected the creation of new sui generis causes of action, favoring instead the extension of existing doctrines, as the State v. Loomis case shows with respect to due process.First, there has been a consistent pattern of courts across jurisdictions favoring extension of existing doctrine conferring interim protection, but also producing uneven and sometimes ill-fitting results such as in the due process case of State v. Loomis. Second, in most jurisdictions where there is no specific AI legislation, data protection law serves as the de facto general regulatory framework for AI the strength, scope and enforcement of which are likely to be the most significant factors shaping the adequacy of AI governance in any given jurisdiction today. Third, the European Union's Artificial Intelligence Act is a signpost of the transition towards purpose-built, risk-graded regulation of AI and its extraterritorial application means it will

likely have an impact, just like the GDPR did before, extending beyond the territorial boundaries of the EU.

An important takeaway for law departments, lawyers and policymakers is that AI law must not be taught, litigated, or legislated as a standalone body of law, but rather as a lens through which other areas of law, such as privacy law, tort law, constitutional law and regulatory theory, are tested and refined. Forced together in this paper are cases and statutes from Illinois and biometric litigation, Indian constitutional jurisprudence, Wisconsin and criminal sentencing, Californian and employment technology and pan-European and risk regulation – to show that the law's response to AI is not concrete and consistent, but rather is being built, case-by-case and statute-by-statute, in real time.

REFERENCES

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).
2. State v. Loomis, 881 N.W.2d 749 (Wis. 2016).
3. Rogers v. BNSF Railway Co., No. 1:19-cv-03083 (N.D. Ill. 2022).
4. Illinois v. Clearview AI, Inc., settlement and consent decree, N.D. Ill. (2022).
5. Mobley v. Workday, Inc., No. 4:23-cv-00770 (N.D. Cal. 2024).
6. Jones v. Peloton Interactive, Inc., No. 23-cv-1082-L-BGS, 2024 U.S. Dist. LEXIS 118511 (S.D. Cal. July 5, 2024).
7. Ryan v. X Corp., No. 24-cv-03553-WHO, 2024 U.S. Dist. LEXIS 222459 (N.D. Cal. Dec. 9, 2024).
8. Taylor v. ConverseNow Technologies, Inc., N.D. Cal. (California Invasion of Privacy Act class action).
9. Walters v. OpenAI, L.L.C., Superior Court of Gwinnett County, Georgia (2023) (AI-generated defamation claim).
10. Federal Trade Commission v. Facebook, Inc., Stipulated Order for Civil Penalty and Injunctive Relief, No. 1:19-cv-02184 (D.D.C. 2019).
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
12. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
13. Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final.
14. Directive (EU) 2024/2853 of the European Parliament and of the Council on liability for defective products.
15. Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
16. Information Technology Act, 2000, No. 21 of 2000 (India), ss. 43A, 72A.
17. California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act of 2020.
18. Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 et seq. (2008).
19. Lei Geral de Proteção de Dados Pessoais (LGPD), Law No. 13,709/2018 (Brazil).

20. White House Office of Science and Technology Policy, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People (Oct. 2022).
21. Exec. Order No. 14,110, Safe, Secure and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75,191 (Oct. 30, 2023).
22. NITI Aayog, National Strategy for Artificial Intelligence: #AIforAll (Government of India, 2018).
23. California Privacy Protection Agency, Automated Decision-Making Technology Regulations, Cal. Code Regs. tit. 11 (finalised 2025).
24. Harry Surden, Values Embedded in Legal Artificial Intelligence, University of Colorado Law Legal Studies Research Paper No. 17-22 (2017).
25. Araz Taeihagh & Hazel Si Min Lim, Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity and Industry Risks, 39(1) Transport Reviews 103-128 (2019).