
ARTIFICIAL INTELLIGENCE AND THE LAW: CHALLENGES OF LIABILITY AND REGULATION IN A TECH-DRIVEN WORLD

By- S. Lavanya¹

ABSTRACT

The rapid rise of Artificial Intelligence (AI) in key areas of our lives—like self-driving cars, predictive policing, healthcare diagnostics, and algorithmic governance—has sparked a serious re-evaluation of legal systems around the globe. While AI brings incredible efficiencies and capabilities, it also poses significant challenges to established legal principles, particularly those related to liability, accountability, and regulatory oversight. Traditional legal frameworks, which were mainly built around human intent and control, seem increasingly out of touch with the decentralized, opaque, and ever-evolving nature of AI. This research paper takes a hard look at the shortcomings of our current legal structures in managing harm caused by AI and the uncertainty surrounding regulations. It highlights how fault-based liability systems struggle when it comes to autonomous technologies, especially when there are no human actors involved in the decision-making process. The paper also explores alternative legal strategies, such as product liability, strict liability, and the emerging concept of “electronic personhood.” It argues that while product liability can offer some solutions, it falls short for AI systems that learn and adapt after deployment, often in unpredictable ways.

Additionally, the paper provides a comparative legal analysis across different jurisdictions. It examines the European Union’s Artificial Intelligence Act, which introduces a risk-based regulatory framework that categorizes AI systems by risk level and requires transparency, oversight, and mechanisms for redress. The paper also looks at India’s policy-driven approach, spearheaded by NITI Aayog, which promotes responsible and inclusive AI but lacks binding

¹Intern, Lex Lumen Research Journal.

authority. The fragmented regulations in the United States, which rely on tort law and consumer protection frameworks, are also scrutinized for their effectiveness in practice.

The study underscores the pressing need for a flexible, adaptive legal framework that can keep pace with the rapid advancements in AI technology.

KEYWORDS: Artificial Intelligence (AI) -Legal Liability-Regulation and Governance-Product Liability Law-Autonomy and Opacity-AI Personhood-Human Rights and Privacy-Comparative Legal Frameworks

INTRODUCTION:

Artificial Intelligence (AI) has transitioned from a concept of the future to a reality that's woven into many aspects of our lives today, from healthcare and transportation to finance, law enforcement, and governance. We're seeing AI technologies—like machine learning, natural language processing, and computer vision—taking on roles that have significant legal, ethical, and societal implications. These systems are now diagnosing illnesses, approving loans, monitoring activities, and even driving cars. As they gain more autonomy and complexity, they're challenging our fundamental legal assumptions, especially around agency, responsibility, and accountability. Legal principles that have long relied on human intentions, foresight, and moral agency are now facing unique hurdles when it comes to AI. A major concern is figuring out who is liable. If an AI-operated vehicle gets into an accident or if an algorithm used in sentencing leads to unfair results, we're left wondering: who is legally responsible? Is it the developer, the manufacturer, the user, or the AI itself? Traditional legal concepts like negligence, product liability, and strict liability fall short when harm occurs without direct human action or when the cause-and-effect relationships are unclear. Additionally, AI systems often act as "black boxes," making decisions based on vast data sets and deep learning methods that even their creators might not fully grasp. This brings up serious issues regarding transparency, explainability, and the right to a fair hearing—key elements of legal and constitutional rights. There's even been talk about granting legal personhood to AI

entities, similar to corporations, especially in discussions within the European Union, raising questions about whether non-human entities should have rights and responsibilities under the law. This paper seeks to delve into the liability and regulatory challenges that AI systems present in today's legal landscape.

UNDERSTANDING THE LEGAL PROBLEM OF AI:

Characteristics of Artificial Intelligence Challenging Legal Norms:

To truly grasp the legal challenges that Artificial Intelligence (AI) brings to the table, we need to dive into its unique technical and functional traits. Unlike the traditional software or automated tools, we're used to, today's AI systems are complex and dynamic, which puts a strain on our existing legal frameworks. Four key characteristics—autonomy, opacity, unpredictability, and scalability—create fundamental issues when it comes to assigning liability, regulatory oversight, and legal accountability. These traits make AI a distinct technological phenomenon that calls for a fresh look at our core legal principles.

a. **Autonomy: The Detachment from Human Control**

AI systems are becoming more autonomous, meaning they can make decisions and take actions without needing real-time human input. Once they're up and running, advanced AI models—especially those that utilize machine learning and neural networks—can process information, adjust their behaviour, and produce results without constant supervision from human operators. This level of autonomy challenges the traditional legal assumption that a human is always in control of potentially harmful activities.

In tort law, particularly under negligence and strict liability principles, determining fault usually depends on the actions or inactions of a person or legal entity. However, when AI operates independently, tracing the causality chain becomes a tricky business. It raises questions about whether liability should fall on the AI's designer, developer, deployer, or user—or if the AI system itself could be held liable, which opens up a whole new can of worms regarding personhood and agency in the legal realm.

There's still a lot of debate among courts and scholars about whether this autonomy is enough to warrant legal personhood for AI. The European Parliament's 2017 resolution hinted at the possibility of recognizing "electronic persons" for highly autonomous systems, but this idea remains contentious and largely untested in legal settings.

b. Opacity: The 'Black Box' Problem

Opacity is all about the challenge—or sometimes the impossibility—of figuring out how AI systems arrive at their decisions. This is especially true for deep learning systems, where even the developers might struggle to trace the exact reasoning that led to a specific outcome. This "black box" characteristic creates major obstacles for accountability, transparency, and due process, particularly in sensitive areas like criminal sentencing, financial choices, and public governance.

Take, for example, the case of *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016). Here, the use of a proprietary AI risk assessment tool in sentencing was questioned on due process grounds, shining a light on the lack of transparency and explainability surrounding algorithmic decisions in the criminal justice system. While the court recognized the concerns, it ultimately upheld the tool's use, citing insufficient proof of harm—leaving lingering questions about constitutional protections in the realm of algorithmic governance. Opacity also creates challenges in administrative law, which often mandates that individuals receive explanations for decisions that impact their rights. If a government agency leans on an AI system to make or assist in decisions but can't clarify how it reached its conclusions, it risks undermining the legal standards for procedural fairness and reasoned decision-making.

c. Unpredictability: The Evolution of AI Post-Deployment

AI systems, particularly those that use unsupervised or reinforcement learning, have the ability to change and adapt over time. They can tweak their internal processes based on new data or real-world interactions. This evolution makes their behavior tough to predict, even for the very people who designed them. Consequently, AI systems might inflict harm in ways that were neither intended nor foreseeable when they were first deployed.

The idea of foreseeability is crucial in most tort laws, especially when it comes to establishing negligence or a duty of care. If the harm caused by an AI wasn't something a reasonable person could have anticipated, it complicates the legal landscape significantly. Navigating the legal landscape when it comes to holding a party accountable under current laws can be quite tricky. On top of that, the unpredictable nature of AI makes it tough to rely on ex-ante regulation, which is all about anticipating and preventing risks before they actually happen.

This unpredictability also stirs up complications in contract law, particularly when AI agents are involved in creating or fulfilling contracts. If an AI system takes it upon itself to enter into or change agreements based on unexpected logic or mistakes, it could lead to disputes over how those contracts should be enforced or interpreted.

d. Scalability: Cross-Border and Mass Impact of AI

Unlike traditional products or services, AI systems can be rolled out on a massive scale, quickly influencing large groups of people across different regions. Just one facial recognition tool or content moderation algorithm can affect millions of users around the world. This situation not only raises legal questions but also jurisdictional ones, as harm can cross national borders, bringing with it a mix of conflicting legal systems, data privacy laws, and liability standards.

This aspect makes it more complicated to enforce rights and seek remedies. Those who suffer from AI-related harm might struggle to figure out where to file their legal claims or who the responsible party is, especially when AI services are provided through cloud platforms or by multinational corporations.

Moreover, the scalability of AI heightens the risk of widespread harm—think algorithmic bias, mass surveillance, or the spread of misinformation. In these scenarios, the damage isn't just individual; it's systemic and widespread, making it even more challenging to pinpoint liability or assess damages under the current private law frameworks.

THE CHALLENGES OF LIABILITY IN AI SYSTEMS:

One of the biggest legal headaches when it comes to Artificial Intelligence (AI) is figuring out who's responsible when these systems cause harm. Traditional liability laws—especially in tort—are built on principles that focus on human actions, like fault, foreseeability, and intent. But the way AI operates, with its autonomous and adaptive features, makes it tricky to apply these old legal standards. In this section, we'll dive into three main approaches to liability—fault-based liability, product liability, and strict liability—specifically in the realm of AI, looking at how effective they are and where they fall short.

A. Fault-Based Liability and Its Limits:

In traditional tort law, to hold someone liable for harm, you need to show that there was a duty of care, a breach of that duty, causation, and actual harm. The key idea, established in the landmark case *Donoghue v. Stevenson*, [1932] AC 562 (HL), is that people have a duty to care for those who might reasonably be affected by their actions. However, fault-based liability relies on the assumption that there are human actors with intentions or negligent behavior - an assumption that doesn't quite fit when AI is in the picture.

a. No Human Actor:

When an autonomous AI system causes harm, it can be tough to pinpoint a direct human responsible at the moment of the incident. Take, for example, a self-driving car that fails to spot a pedestrian and ends up causing an injury. Who should be held liable? Is it the car manufacturer, the developer of the AI software, the provider of the data set, or the end user who simply activated the system?

Traditional tort law expects there to be a defendant whose actions can be measured against the standard of reasonable care. But with AI, decisions often come from a mix of inputs and algorithmic processes that no single person controls, making it hard to determine who holds the duty and who breached it.

b. Absence of Mens Rea:

When it comes to fault-based liability, the focus is on proving intent or negligence. But here's the catch: AI systems don't have mental states or moral agency. They don't "intend" outcomes in the way we think of it legally. This absence of a

conscious actor makes it tough for courts to determine if there was a breach of duty due to intent or carelessness.

Mens rea is crucial in criminal law, and it also plays a key role in civil liability. If it turns out that no one acted negligently and the AI operated without any human input, then fault-based liability could completely fall apart—leaving those who were harmed with no way to seek justice.

B. Product Liability Approach:

As fault-based models show their limitations, many scholars and courts are shifting their focus to product liability, which introduces the concept of strict liability for defective products. This means that proving negligence isn't necessary; all that needs to be established is that a product was defective and caused harm.

a) Design and Manufacturing Defects:

According to this doctrine, a manufacturer can be held strictly liable if an AI product is found to be defectively designed or manufactured. However, AI systems—particularly those that utilize machine learning—can change after they've been deployed, adapting their behavior based on new data inputs. An AI might perform safely during testing but could develop unsafe responses when faced with real-world scenarios. This ability to learn complicates the traditional idea of “design” as it was understood at the time of manufacture.

Figuring out whether a “defect” existed at the point of sale becomes a legal gray area when harmful behavior only surfaces after the system has adapted beyond its original programming.

b) Failure-to-Warn Liability:

Another key aspect of product liability is the obligation to inform users about foreseeable risks. Courts have consistently ruled that manufacturers must warn consumers about dangers that come with using their products. However, with AI, many risks may not be apparent at the time the product is distributed. For instance, if an AI system starts making biased decisions based on real-world prejudices found

in its training data, it's uncertain whether such behavior could have been anticipated or warned against.

C. Strict Liability and Enterprise Risk:

Additionally, even if the risks were foreseeable, effectively communicating them can be a challenge due to the complex nature of AI systems and their rapid evolution.

When it comes to addressing legal gaps, some scholars suggest we should consider a strict liability model based on enterprise risk theory. This means that any party involved in a risk-generating activity—like using an AI system—should be held responsible for any harm it causes, no matter their level of fault or intent.

The reasoning behind this is all about economic efficiency and fairness. Those who profit from AI should also take on the costs associated with it, including any external damages. This approach encourages companies to invest in safety, transparency, and thorough testing.

On the flip side, critics warn that strict liability could stifle innovation, especially for startups and smaller businesses that might not have the resources to handle extensive and unpredictable liabilities. Striking the right balance between promoting technological advancement and ensuring that victims are compensated is a tricky and ongoing challenge.

LEGAL PERSONHOOD FOR AI?

As Artificial Intelligence (AI) continues to grow in both complexity and independence, there's an increasing interest in the legal world about whether these systems should be recognized as having limited legal personhood. The idea behind this is to allow AI entities to have rights, responsibilities, and—most importantly—accountability when they cause harm. This approach aims to fill the current gap in liability, where no one person is clearly responsible for the actions of these autonomous systems.

1. European Parliament Proposal: The Concept of “Electronic Persons”

This proposal ignited a lively debate among legal and ethical experts. Supporters argued that granting legal personhood would create a clear framework for liability, enabling AI systems to be held accountable through insurance or trust funds set up at the time of their deployment. On the flip side, critics were vehemently against the idea, claiming it would undermine human accountability and lead to moral ambiguity. They pointed out that legal personhood typically assumes some level of moral reasoning or intent—traits that AI systems simply do not possess.

2. The Corporate Analogy and Its Limits

When people talk about AI being treated like a legal person, they often bring up corporations as a comparison. Corporations are these artificial entities that the law recognizes as having personhood, even though they don't have a physical presence or consciousness. But this analogy has its flaws. At the end of the day, corporations are made up of people who are held accountable for what the corporation does, thanks to legal concepts like vicarious liability and fiduciary duty.

On the flip side, AI systems don't have the same human oversight or governance. They lack the ability to make decisions based on moral judgment or institutional guidelines. Without human conscience, intent, or a sense of social responsibility, treating AI as a legal person could blur the lines of accountability and challenge the very foundations of justice we rely on.

GLOBAL REGULATORY RESPONSES:

As Artificial Intelligence (AI) systems become more and more common, countries around the globe are stepping up to regulate their risks and ensure accountability. While the methods differ from one legal system to another, there's a growing agreement on the importance of transparency, fairness, and public safety. This section takes a closer look at the regulatory frameworks in three key regions—the European Union, the United States, and India—to see how these legal systems are tackling the challenges that AI presents.

1. European Union: The Artificial Intelligence Act

The AIA takes a risk-based approach, categorizing AI systems into four groups: unacceptable risk, high-risk, limited risk, and minimal risk.

Some of the key features of the Act:

- Transparency obligations, especially for systems that interact with people, create deepfakes, or provide recommendations.
- Bans on AI applications considered to pose unacceptable risks, including social scoring, real-time biometric surveillance, and subliminal manipulation.

2. United States: Sectoral and Case-by-Case Regulation:

The AIA embodies a precautionary regulatory model that prioritizes fundamental rights, consumer protection, and democratic oversight over mere economic interests. It showcases the EU's commitment to ensuring that digital technologies uphold human dignity and the rule of law. However, some critics point out that the compliance requirements might stifle innovation, particularly for small and medium-sized enterprises.

Notable instruments include:

When we look at how the United States handles AI regulation, it's quite different from the EU's more unified approach. As of 2025, there's no all-encompassing federal law governing AI in the U.S. Instead, the landscape is a patchwork of administrative guidelines, proposed laws, and court rulings.

Some key elements include:

- The Federal Trade Commission (FTC) has put forth guidelines aimed at preventing algorithmic bias, ensuring data integrity, and fostering transparency in how AI is used.
- The Algorithmic Accountability Act, which first made its debut in 2019 and has been reintroduced in subsequent Congressional sessions, calls for

impact assessments on AI systems. Unfortunately, this bill hasn't been passed yet.

- Court rulings, especially those related to facial recognition technology, show how constitutional rights—like those in the Fourth and Fourteenth Amendments—are being used to challenge AI tools that may be discriminatory or invasive.
- Moreover, Section 230 of the Communications Decency Act limits the liability of online platforms for third-party content, which complicates holding them accountable for AI-driven content moderation or recommendation algorithms.
- While this flexible approach in the U.S. encourages innovation, it often falls short in providing clear protections or rights for individuals impacted by AI systems. The regulatory gaps can lead to inconsistent court interpretations and a lack of avenues for seeking justice.

3. India: Emerging Ethical and Policy Frameworks:

As of 2025, there isn't any binding legislation specifically focused on AI, but discussions around policy have picked up pace in recent years. A significant step forward is the NITI Aayog's "Responsible AI for All" strategy paper, which lays out principles and suggestions for developing AI in an ethical and inclusive manner.

The document puts forward several recommendations:

- Setting up an AI oversight board to review and guide the ethical application of AI across various sectors.
- Creating guidelines to reduce algorithmic bias, improve explainability, and ensure fair outcomes for everyone.
- Establishing sector-specific regulatory sandboxes to safely test AI technologies under supervision.

India's approach highlights the importance of human-centric development, resonating with the constitutional ideals of equality and dignity found in Articles 14 and 21 of the Indian Constitution. However, the absence of enforceable regulations means that the current framework remains largely aspirational. Additionally, there are ongoing concerns about the use of AI in public surveillance, welfare targeting, and law enforcement, which continue to raise important questions about constitutional rights and civil liberties.

CONSTITUTIONAL AND HUMAN RIGHTS CONCERNS:

The rise of Artificial Intelligence (AI) in areas like public governance, law enforcement, and private sector decision-making brings up some serious constitutional issues. We need to pay close attention to how AI might infringe on our fundamental rights—especially when it comes to privacy, equality, and due process. As AI systems become more autonomous and less transparent, making sure they comply with our constitutional rights is both challenging and crucial.

1. Privacy and Surveillance

AI technologies, especially those that involve facial recognition, biometric tracking, and behavior prediction, can seriously threaten our constitutional right to privacy. These surveillance tools, often used by the state, can lead to mass tracking of individuals without their knowledge or consent, creating a chilling effect on our civil liberties.

The Court highlighted that having control over personal data is essential to our personal liberty and dignity. AI systems that collect and analyze personal data—often without clear consent—risk breaching this constitutional standard. Technologies like facial recognition systems (FRS) and predictive policing tools can disproportionately target marginalized communities, increasing the risks of over-policing and discrimination based on surveillance. The absence of legal protections for the use of such technologies in India only makes the situation worse.

In democratic societies, we must find a way to balance AI's surveillance capabilities with our constitutional protections through data protection laws, judicial oversight, and ensuring.

2. Bias and Discrimination:

One major constitutional issue we face is algorithmic bias. When AI systems are trained on historical or biased data, they can reinforce and even worsen existing social prejudices, particularly in critical areas like criminal justice, employment, creditworthiness, and healthcare. Take the case of *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), where the defendant contested the use of a proprietary AI tool called COMPAS in his sentencing. The tool's unclear algorithm made it impossible for him to challenge the factors that contributed to his high-risk score, raising serious concerns about his due process rights.

Using AI for decision-making without proper systems for explanation, accountability, or the ability to appeal can undermine the principles of procedural fairness. In places like India, this lack of transparency could clash with the right to equality under Article 14 and the right to a fair trial under Article 21.

To tackle this problem, we need proactive regulations that require bias audits, clear explanations, and appeal processes in AI applications. Moreover, courts should establish legal standards that hold both public and private entities responsible for any discrimination caused by AI.

RECOMMENDATIONS FOR LEGAL REFORM:

The rapid evolution of Artificial Intelligence (AI) demands a thoughtful and flexible legal approach. While our current legal frameworks provide a solid foundation, they often fall short when it comes to tackling the distinct challenges posed by autonomous and complex technologies. To maintain the rule of law, protect individual rights, and foster technological progress, we need a comprehensive strategy for legal reform.

a. Collaborative Regulation:

When it comes to AI regulation, we should adopt a collaborative governance model that brings together insights and expertise from a variety of stakeholders:

- Legislators and the Judiciary need to ensure that laws keep pace with technological advancements while safeguarding constitutional rights.

-
- AI Developers and industry experts offer the technical know-how essential for creating practical regulations.
 - Civil Society and Academia play a crucial role in making sure that public interest, fairness, and ethical considerations aren't overshadowed by business objectives.

This approach aligns with global best practices, like the OECD Principles on Artificial Intelligence (2019), which emphasize the importance of inclusive policy-making through multi-stakeholder collaboration.

b. Risk-Based Regulatory Frameworks:

A one-size-fits-all legal strategy simply won't work in the realm of AI. The European Union's Artificial Intelligence Act serves as a valuable example by classifying AI systems based on their risk levels: unacceptable, high-risk, limited-risk, and minimal-risk.

This tiered system ensures that:

- High-risk applications (like biometric surveillance and healthcare AI) undergo thorough evaluations.
- Low-risk applications (such as spam filters) are subject to lighter regulations.
- Countries like India and other emerging economies can implement a similar framework, customized to fit their unique social and technical landscapes.

c. Legal Sandbox Models:

To strike a balance between fostering innovation and ensuring regulatory oversight, governments should consider implementing regulatory sandboxes.

For instance, the United Kingdom's Information Commissioner's Office (ICO) has already taken the lead by piloting AI sandboxes to assess privacy, transparency, and fairness in algorithmic processing. These models provide:

- Real-time monitoring of AI applications
- Early detection of potential harms
- A flexible space for rulemaking

Such frameworks can be tailored for various sectors, including healthcare, fintech, and criminal justice, both in India and beyond.

d. Explainability Mandates:

Legal systems ought to require that AI systems are explainable or auditable. While achieving full interpretability might be a tall order with complex neural networks, the law can still mandate:

- Post hoc explanations
- Impact assessments
- Audit trails

This approach aligns with due process requirements and upholds the constitutional right to reasons under administrative law.

Explainability mandates are crucial for enabling legal recourse, ensuring accountability, and maintaining public trust in automated decision-making.

e. Updating Liability Laws

It's essential to modernize traditional tort and product liability doctrines to reflect the complex and evolving nature of AI-related harm.

- **Shared Liability Models:** These would allow multiple parties—developers, deployers, and data providers—to share responsibility based on their level of control and profit from the system.
- **Insurance Mechanisms:** We should establish mandatory AI insurance markets to efficiently compensate victims, similar to how motor vehicle insurance operates.
- **Rebuttable Presumptions:** Introduce legal presumptions that shift the burden of proof to AI operators once harm from autonomous systems is established.

CONCLUSION:

The emergence of Artificial Intelligence (AI) isn't just a tech revolution; it's a pivotal moment for our legal systems. AI systems, which can make decisions on their own, learn continuously, and operate on a massive scale, bring about challenges we've never faced before in the realm of law.

Unlike traditional agents, AI doesn't have consciousness, intent, or moral responsibility, yet it significantly impacts our fundamental rights, public safety, and the fabric of our economy. Current legal frameworks—whether they focus on fault-based torts, strict liability, or product liability—were designed for a world where human actions and predictability were the norm. These systems struggle when faced with complex “black box” algorithms or self-driving cars that make quick decisions without human input. Take the case of *Donoghue v. Stevenson*, [1932] AC 562 (HL), for example; tort law has historically tied liability to human foresight and reasonableness—ideas that don't easily apply to the fast-evolving, data-driven technologies we see today. Given these challenges, our legal responses need to be both creative and principled. Looking at regulatory trends around the world—like the European Union's AI Act, the FTC's guidelines on algorithmic fairness in the U.S., and India's NITI Aayog framework—it's clear that regulations tailored to specific sectors, based on risk, and grounded in human rights are becoming more popular. However, without a unified global approach, we risk creating a patchwork of laws that could lead to regulatory arbitrage, where companies move to places with looser regulations, ultimately weakening the rule of law and international collaboration.

To tackle this, we need to harmonize laws across borders, founded on shared values like transparency, accountability, and fairness. Additionally, legal innovation should embrace flexible regulatory models such as regulatory sandboxes, frameworks for auditing algorithms, and standards for explainability, all while safeguarding essential constitutional rights—especially the right to privacy, equality, and due process. It's essential that the law doesn't just react to changes but stays ahead of the curve when it comes to technological advancements. We need a legal framework that's proactive, driven by foresight, ethical considerations, and democratic values. As AI systems increasingly influence areas like public policy, criminal justice, job hiring, and financial access, our legal system must prioritize human dignity and democratic oversight over mere technological ease. In short, while AI holds incredible promise for society, it needs to be integrated into a legal framework that emphasizes human rights, accountability, and the public good. Only then can we ensure that law and technology progress together towards a fair, just, and human-focused digital future.

REFERENCES:

1. European Commission, Proposal for a Regulation on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final.
2. European Parliament, Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics, 2015/2103(INL).
3. NITI Aayog, Responsible AI for All: Strategy Paper (2021), available at <https://www.niti.gov.in>
4. Restatement (Third) of Torts: Products Liability § 2 (Am. L. Inst. 1998).
5. John R. Searle, Minds, Brains and Programs, 3 Behav. & Brain Sci. 417 (1980).
6. Donoghue v. Stevenson, [1932] AC 562 (HL).
7. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
8. State v. Loomis, 881 N.W.2d 749 (Wis. 2016).
9. Federal Trade Commission, Aiming for Truth, Fairness, and Equity in Your Company's Use of AI (2021), <https://www.ftc.gov>