Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Legal Liability for AI-Driven Data Breaches

Article History:

Name of Author:
Melinda Mccoy[1], Brenda Perez[2], Susan Sutton[3], Sherry Walker[4] and Lindsey Sloan[5]

Affiliation: [1]Professor, Department of Corporate Governance, Transatlantic Management School, Germany
[2]Research Associate, School of Retail Management, Alpine Institute of Technology, Switzerland
[3]Academic Coordinator, Department of Business Analytics, Balkan University of Technology, Serbia
[4]Academic Coordinator, Department of Banking and Insurance, Avalon State University, USA
[5]Professor, School of Economics and Commerce, Nairobi Metropolitan University, Kenya
Corresponding Author: Melinda Mccoy

How to cite this article: Melinda Mccoy, *et, al*. Legal Liability for AI-Driven Data Breaches. *J Community Med* 2021;2(1);42-45.

Abstract: As artificial intelligence (AI) becomes increasingly autonomous and central to modern data infrastructure, the incidence and complexity of AI-driven data breaches have risen dramatically. Such breaches challenge traditional notions of legal responsibility, attribution, and regulatory oversight. This article analyzes the evolving legal landscape for liability in AI-oriented data breaches, exploring regulatory trends, emerging case law, compliance challenges, technical pitfalls, and transnational enforcement. The discussion is enriched by recent data, sectoral statistics, and visual illustrations of global regulatory readiness and breach trends.

Keywords: AI-driven data breaches, Legal liability, Regulatory oversight, Compliance challenges, Transnational enforcement,

INTRODUCTION

AI is now woven into the fabric of global commerce and critical infrastructure, automating decision-making, personalizing customer experience, and managing vast pools of sensitive data. The downside: AI amplifies vulnerabilities—whether through autonomous error, flawed training, or malicious code—turning data breaches into both a legal and operational minefield.

Key questions include:

- Who is legally responsible when an AI system causes or enables a data breach?
- Are developers, deployers, or data controllers liable—or does liability depend on context?
- How do evolving regulations and case law address attribution, causation, and damages?

Nature and Scale of the Threat

AI-driven data breaches encompass:

- Direct cyberattacks or unauthorized access enabled by weak AI controls.
- Data exfiltration via AI-enabled malware or adaptive ransomware.
- Privacy violations from AI "black boxes" misprocessing personal data.
- Attacks targeting AI models themselves, such as poisoning or adversarial manipulation.

Statistics from 2025 reveal:

- **87% of global organizations have faced an AI-powered cyberattack in the past year**.
- Projected losses from such attacks may exceed $18.6billion globally by year-end.
- Financial firms average regulatory penalties of $35.2million per AI compliance failure[1][2].

Regulatory Backdrop and Evolving Laws

1. General Data Protection Regulation (GDPR, EU/EEA)

- GDPR applies strict liability for data controllers and processors in data breach situations, even when AI is involved.
- Article 82 enables compensation claims for both material and non-material damages following GDPR violations, including data breaches linked to AI systems.
- Enforcement actions and fines are becoming more frequent and substantial[3][4].

2. The EU AI Act (mid-2025)

- Introduces transparency, risk, and documentation obligations for AI developers and deployers.
- Particularly stringent for high-risk AI systems in sectors such as healthcare, finance, and critical infrastructure[5].

3. Digital Operational Resilience Act (DORA)

- Imposes mandatory reporting and accountability for ICT risks, including AI, across the EU finance sector, effective Jan. 2025.

4. United States

- Patchwork of state-level privacy statutes, with strict liability emerging for mishandling and downstream vendor breaches (e.g., California, Delaware, Tennessee, Minnesota, Maryland—enacting new laws in 2025)[6].
- Federal laws cover health, finance, and children's data, but there is no comprehensive AI liability statute yet.

5. India and Asia-Pacific

- India's new Digital Personal Data Protection Act and discussions around an Artificial Intelligence and Data Ethics Act are closing regulatory gaps.
- China, Singapore, South Korea, and Japan are expanding AI-specific compliance and auditing rules[7][8].

[image:1]

Figure 1: Region-wise regulatory readiness for AI data breach liability (2025).

Legal Attribution and Stakeholder Liability

AI-driven data breaches blur the lines on legal attribution. Liability may fall on:

- **AI Developers/Providers:** If flawed design, inadequate testing, or bias in algorithms is proven.
- **Deployers/Operators:** For failures in implementation, oversight, or compliance with data security standards.
- **Third-Party Vendors:** Especially if data is processed on their systems and they fail in their duty of care.

Legal standards are evolving:

- **Product Liability** is being adapted for autonomous AI: Some courts consider AI-led products as "defective" if they lack adequate security safeguards.
- **Negligence** applies if reasonable precautions (like training, monitoring, audit trails) are not observed[9][10].
- **Strict Liability** models are being debated, especially for high-risk or unexplainable ("black box") AI systems[11].

> "With the rapid evolution of AI technology, understanding the legal and regulatory frameworks governing AI-driven data breaches is critical...Examining existing frameworks, real-world cases, and best practices is crucial for mitigating liability."[10]

COMPLIANCE, RISK MANAGEMENT, AND PREVENTION

In response to regulatory and legal demands:

- **Pre-deployment assessments, algorithmic audits, and explainability requirements** are now standard practice.
- Organizations must maintain **incident response plans**, ensure compliance with security and privacy certifications, and report breaches within strict timelines (24 hours under new global rules).
- **Cyber insurance** now often includes explicit coverage for AI-driven breach risks, but insurers demand proactive governance evidence.

Graph: AI-Driven Data Breach Incidents and Legal Actions (2023–2025)

[image:2]
Figure 2: Growth in AI breach incidents and related legal disputes, 2023–2025.

Challenges for Legal Accountability

- **Attribution Complexity:** Difficulty tracing responsibility in multi-actor AI ecosystems, especially with self-learning or external model training[11].
- **Black Box AI:** Courts struggle when causality is obscured by opaque algorithms, especially when intent or foreseeability is hard to prove.
- **Transnational Enforcement:** Global AI systems operate across multiple jurisdictions, often exploiting regulatory inconsistencies[4][7].
- **Class Actions and Collective Redress:** Mechanisms for large-scale consumer/litigant recovery remain weak outside certain EU/US models[3].

Notable Cases and Precedents

- EU courts have set compensation benchmarks for GDPR data breach claims tied to AI (awards range between €500 and €7,500 per non-material damage incident)[3].
- In the US, AI is at the center of growing state-level litigation waves and enforcement actions, with class actions on the rise[6][9].
- India and Asia-Pacific are progressing towards hybrid liability models, factoring in both control and foreseeability by all stakeholders[11].

Future Outlook

Key recommendations and structural priorities:

- **Adaptive, AI-specific laws**: Governments are urged to mandate algorithmic transparency, implement AI impact assessments, and consider strict liability for high-risk systems[4][11].
- **Robust cross-border frameworks**: Multilateral cooperation to harmonize standards and close regulatory loopholes.
- **Best practice guidance**: Agencies such as CISA and the EU Commission publish evolving guidance on AI system security, data governance, and incident response[12].
- **Ethical AI:** Stronger requirements for data minimization, user rights to explanation and redress, and mandatory auditing for discrimination or harm.

CONCLUSION

Legal liability for AI-driven data breaches is a moving target, caught between technological innovation and the imperative for user protection. The world's leading economies now recognize the unique challenge posed by AI's autonomy, opacity, and scale, and are gradually shaping a regime that combines strict duty of care, transparency mandates, and co-liability across the AI supply chain. For organizations, proactive risk management, legal compliance, and ethical stewardship of AI are no longer optional—they are the frontline defense against mounting legal risk.

Figures & Visuals

- Region-wise Regulatory Readiness for AI Data Breach Liability (2025)[image:1]
- AI-Driven Data Breach Incidents and Related Legal Actions (2023–2025)[image:2]

[image:1]
[image:2]

REFERENCES

1. https://community.nasscom.in/communities/ai/ai-vs-ai-cybersecurity-arms-race-2025
2. https://www.metomic.io/resource-centre/quantifying-the-ai-security-risk-2025-breach-statistics-and-financial-implications
3. https://www.dentons.com/en/insights/articles/2025/july/14/challenges-in-establishing-liability-for-ai-driven-products
4. https://juriscentre.com/2025/04/17/ai-and-data-driven-breaches-legal-challenges-and-liability-frameworks/
5. https://bigid.com/blog/2025-global-privacy-ai-and-data-security-regulations/
6. https://www.jacksonlewis.com/insights/year-ahead-2025-tech-talk-ai-regulations-data-privacy
7. https://lumiversesolutions.com/data-privacy-new-laws-in-2025-whats-changing-copy/
8. https://iclg.com/practice-areas/data-protection-laws-and-regulations/02-ai-regulatory-landscape-and-development-trends-in-china
9. https://www.connkavanaugh.com/articles-and-resources/what-every-business-should-know-about-ai-in-2025-legal-perspectives-and-predictions/
10. https://thebarristergroup.co.uk/blog/ai-data-breaches-and-liability-whos-responsible

11. https://ijlr.iledu.in/the-legal-and-ethical-implications-of-ai-driven-data-breaches-challenges-in-attribution-and-liability/
https://www.insidegovernmentcontracts.com/2025/06/cisa-releases-ai-data-security-guidance/