Artificial intelligence in the supply chain: Legal issues and compliance challenges

Received (in revised form): 9th August, 2024

Samuel G. Kramer

SAMUEL G. KRAMER
Partner, Baker & McKenzie, USA

Samuel Kramer is a Partner in the Commercial, Data, IPTech and Trade (CDIT) Group in the Chicago office of Baker & McKenzie. A graduate of Northwestern Pritzker School of Law, Sam's practice focuses on structuring and negotiating outsourcing and managed services arrangements. He regularly advises companies in complex licensing, technology-related agreements and commercial supply chain contracts. Sam is a frequent speaker and writer on emerging technologies in the law, including blockchain and artificial intelligence (AI). He is the US coordinator of the company's FinTech and blockchain practices. Sam is recognised by Chambers Global and Chambers USA for technology and outsourcing and is in the Legal 500 Hall of Fame for technology and outsourcing. He is also an Acritas Star lawyer.

Baker & McKenzie LLP, 300 East Randolph Street, Suite 5000, Chicago, IL 60601, USA
Tel: +1 312 861 7960; E-mail: samuel.kramer@bakermckenzie.com

Abstract

Driven by the rise of Big Data and improvements in computational power, artificial intelligence (AI) solutions are transforming entire industries, including their supply chains. These technologies can leverage the collection of data across a wide variety of supply chain sources, bringing optimisations to everything from customer engagement to business intelligence, but they are not without risks. The process of implementing AI into supply chain management practices can easily lead to noncompliance without a robust data governance strategy at a company level. In order to mitigate these risks, as well as ensure standards of safety and quality, a critical examination of all AI technologies across their entire life cycle is required. This paper serves to outline recent developments in AI technology and how they have been implemented in supply chain management across industries. The risks of implementing AI solutions in the supply chain are discussed through case studies as well as recent litigation involving breaches of data privacy laws, licensing agreements and other liability stemming from inappropriate use of AI technologies. A summary of the current state of AI law and policy in the US and European Union (EU) serves as a basis for recommendations for adoption of responsible AI practices. Through the establishment of AI governance frameworks that assess risks at all stages of the implementation process, AI solutions can be designed and implemented that are reliable, secure and resilient.

Keywords

artificial intelligence, supply chain, legal compliance, AI legislation

DOI: 10.69554/AWRA2732

INTRODUCTION

Artificial intelligence (AI) has been developing in computer science since the term was coined at a research programme in 1956. In the following decades, AI progressed with the development of new

algorithms to address problem solving and interpretation of spoken language. But the lack of computational power and computer storage were major obstacles to creating artificial decision-making systems. While increasing computer power over time gave us thinking machines, such as IBM's Deep Blue that could defeat the world's best chess players, and consumer-level speech recognition products, like Dragon Naturally Speaking software, this traditional AI was limited by a lack of input data and was still constrained by the computational weakness of on-premises computer systems.

Today we live in the age of big data. By the end of 2025, over 180 zettabytes of electronic data will have been created worldwide.[1] At the same time, industry has moved from on-premises computing solutions to the cloud, tapping into the computational assets of extremely powerful data centres that rent their platforms to organisations. These giant cloud computing providers use access to vast stores of data to train algorithms to solve computational problems. More recently, generative AI (GenAI) has burst into public consciousness with OpenAI's release of ChatGPT and GPT 4. These large language models (LLMs) enable businesses to use AI to interact with their customers through chatbots that simulate human interaction. New machine learning (ML) models ingest large amounts of data to output predictive analytics that drive business change.

Businesses are increasing spending on generative AI, but most remain in the testing phase. Some companies, however, have already rolled out targeted GenAI solutions. In retail, GenAI-powered design tools manipulate customer uploaded images to reimagine spaces with company products.[2] In the energy industry, chatbots help calculate a business' carbon emissions.[3] AI enabled diagnostics in healthcare identify patients with similar profiles.[4] The travel industry is using GenAI to personalise the booking process based on travel histories and preferences.[5] These emerging use cases leverage big data-enabled technologies to increase efficiency and improve the customer experience and supply chain management and logistics is no exception.

Data analytics is transforming supply chains by expanding the dataset for analysis beyond the traditional internal data held on enterprise resource planning and supply chain management systems. It also applies powerful statistical methods to both new and existing data sources to generate insights exceeding the capabilities of these traditional systems. Upstream, AI can transform supplier relationships and inventory management through predictive analytics and real-time data processing. Downstream, supply chains benefit from enhanced customer experiences facilitated by AI-driven insights and personalisation.

The leveraging of AI in the supply chain requires robust data management, governance and data usage policies to manage the exposure to legal ramifications arising from AI models, including laws related to the acquisition, handling and use of data, as well as liability for the use of the model's outputs. This paper will describe various use cases where AI solutions have been deployed, and the operational benefits that can be derived from them. Then it will address the legal and compliance risks that can arise from the use of AI in the supply chain. Finally, it will recommend measures to mitigate those risks and manage the exposure from a responsible use of AI in the supply chain.

WHAT IS AI?

AI solutions involve the deployment of algorithms, which can be defined as the sets of programming instructions for processing data or performing some other task. Since its inception in the 1960s, AI has grown in fits and starts. In recent years, the availability of increased computing power, especially in public cloud infrastructure, the development of convolutional neural networks and the wider availability of big datasets allowed AI to overcome previous limitations and deliver real-world solutions to business enterprises.

ML algorithms can process data and make predictions without relying solely on pre-programmed rules. These systems use training data about some known objects or events of a particular category to identify correlations that can be used to make assessments about other objects or events of the same kind. Tuning the algorithm adjusts the weightings assigned to features the algorithm relies on in the dataset to optimise its predictions, resulting in improved quality of its predictions over time.

Deep learning (DL) is a type of machine learning, where algorithms perform tasks previously executed by developers: defining what features in a dataset to analyse and deciding how to weight those factors to deliver an accurate prediction. DL uses neural networks, which are a class of models containing a system of layers interconnected by weights and biases. A neural network analyses inputs and makes a prediction; if the prediction is wrong, the DL algorithm adjusts the weights and biases of the model until prediction accuracy improves.[6]

LLMs are a type of DL algorithm that has been tuned to perform natural language processing (NLP). These models ingest large datasets to classify inquiries and assign statistical relationships from training texts to predict the text to follow. Generative pre-trained transformer (GPT) is a type of LLM that is designed to interpret human language, both written and spoken. GPT systems respond to natural language inquiries, or prompts, and respond to reinforcement from human feedback on the quality of their operations.

Deployment of algorithmic decision making has also been the subject of concerns related to fairness and transparency, particularly in the housing, employment and financial advisory sectors. Those concerns have become a central theme in the criticism of the increasing reliance on AI across industries. In 2022, the U.S. Department of Justice brought an action against Meta, claiming that the vast amount of data it had collected from its users trained its personalisation algorithms to serve housing ads to certain groups of potential consumers, and not to potential consumers in other groups, based on protected classes (such as race, religion, national origin, disability, etc.). Meta quickly settled and agreed to refrain from using certain AI tools and to address bias in its personalisation algorithms.[7]

AI SUPPLY CHAIN USE CASES

Data-driven solutions augmented by AI are in use across all aspects of the supply chain. AI is fundamentally reshaping practices both upstream, encompassing raw material acquisition, manufacturing intricacies and supplier relations, and downstream, embodying distribution strategies, customer engagement and after-sales service.[8] GenAI solutions have been deployed in supplier identification and selection phases. It has

the ability to examine a large volume of data from many potential suppliers across a diverse range of parameters, including cost-effectiveness, product quality, reliability, operational efficiency and sustainability, enabling supply chain managers to curate an optimal supplier portfolio. AI tools can also facilitate the promotion of a company's supplier selection mandates, suggesting strategies to integrate minority-owned, women-owned or veteran-owned enterprises within the supply chain.[9]

AI-enabled supplier selection tools can generate lists of potential new suppliers by scraping websites for data on suppliers' finances, customer ratings, sustainability records, diversity scores, intellectual property ownership information, documentation from customs officials to substantiate international trade experience, public record court records for claims and real-time alerts from social media and news feeds that can be set by the user to include financial reports and major hires or terminations. AI tools can perform deep searches to find pitch decks and identify a prospective supplier's client base to better understand their capabilities. Improving supplier diversity supports a deeper supplier bench and introduces suppliers that can fill holes during disruptions.

In supply chain operations, AI tools can predict demand and formulate a comprehensive strategy for meeting that demand, including sourcing, production, distribution and customer service activities. It enables a dynamism and responsiveness not typically associated with more traditional, rules-based AI systems. AI tools have been deployed to shorten manufacturing lead times and direct material sourcing. These tools can optimise inventory and balance supply and demand, help determine ideal layouts for storage and picking activities within warehouses based upon item-specific demand frequency and merchandise's physical dimensions. AI solutions help to rationalise shelf space and provide real-time data on inventory levels to support just-in-time (JIT) operations.

AI has also transformed supply chain logistics activities. It can analyse vast amounts of real-time data to devise the most efficient transportation routes and provide textual justifications for selected routes, offering logistics managers a broader range of options and facilitating superior decision making.[10] Internet of Things (IoT) sensors with data streams from carriers, ports, airport operations, rail lines, traffic reports and weather forecasts enable predictive and contextualised business intelligence.

Business disruptions from disasters and force majeure events can be mitigated using AI. AI may assist businesses in monitoring and reacting promptly to disruptions that might affect their supply chains. Following the identification of a possible risk, the system can automatically generate and send messages to concerned suppliers. Scenario-based risk assessment exercises that generate potential disruption models, including supplier insolvency, strikes, natural disasters and other disruptions, aid companies in devising resilient strategies and contingency plans to ensure business continuity.

Company policies and ethical sourcing standards can be furthered through the use of AI in the supply chain, supporting the reduction of a company's carbon footprint, eliminating waste and promoting sustainability. AI solutions can prioritise fair trade and ethical sourcing practices. Deployment of AI to scrutinise data from supplier audits, regulatory filings and media reports

can pinpoint potential compliance risks as well as evidencing the achievement of corporate environment, social and governance (ESG) commitments.[11]

AI is not, however, a panacea to cure all that ails a company's supply chain. Business model innovation is a formidable challenge for any organisation, given that returns on investment are not guaranteed and are seldom realised in the short term. The current state of AI has limited comprehension of human cognition, organisational culture and the multi-faceted intricacies that govern business ecosystems. This lack of depth in understanding the nuances of supply chain configurations, stakeholder relationships and cultural dynamics, which is often developed through years of industry experience, constrains the ability of these AI systems to drive organisational change. And where AI simplifies tasks for supply chain managers, it adds significant new decision-making responsibilities.

RISKS OF USING AI

AI solutions require vast amounts of data to function optimally. Generating or acquiring that data can be resource intensive and fraught with legal consequences. Many small and medium-sized enterprises (SMEs) lack robust data management processes, policies and technical infrastructure that can impede the ability to leverage AI responsibly. The absence of stringent data governance exposes an organisation to legal liability, as it may unintentionally violate laws surrounding the use and handling of data, especially personal or sensitive information.

In 2023, a class action lawsuit was filed against OpenAI and Microsoft, alleging that they violated the Computer Fraud and Abuse Act by intentionally accessing protected computers, using scraping and plug-ins to obtain data without authorisation to train their GenAI products, in breach of the website's terms and conditions.[12] This case also alleged violation of data privacy laws through unauthorised use of scraped personal data. ChatGPT was briefly banned in Italy on the concern that the training and retraining of the tool with data scraped from protected websites and the public Internet violated the privacy rights of Italian individuals under the General Data Protection Regulation (GDPR).[13] A similar case was lodged against Alphabet with respect to the acquisition and use of training data for its GenAI product.[14]

Other claims have been made against AI developers with respect to training data. Thomson Reuters, the owners of the Westlaw legal research platform, sued a rival legal database provider for copyright infringement, alleging it copied Westlaw's database to train its own AI legal research product.[15] The *New York Times* and Getty Images have both sued GenAI companies for having infringed their copyrights in news stories and images scraped from their websites and used to train AI models.[16] While these and many other infringement cases are pending, the risks to AI developers and users remain. Training models on improperly acquired data exposes the AI tool provider to a range of claims that not only result in damage awards but may impair or prevent the continued availability of the tool.

For supply chain managers considering implementation of an AI solution, the risks of third-party claims based on the AI tool inputs occur at two levels. The use of AI tools extends the liability surrounding training data to the user, because copying and distribution of infringing data or data that

violates privacy rights can themselves constitute infringing acts and privacy breaches. When licensing AI with pre-trained datasets, companies should obtain express warranties that all data used to train the model was obtained lawfully and receive indemnification for third-party claims that arise from allegations that the collection and use of the input data was unauthorised.

Companies also need to be vigilant in supplying their own training data for AI solutions. Supply chain AI tools may tap into large data stores at a company to provide insights into purchasing patterns, inventory management and other aspects of supply chain operations. Without robust data management policies, companies risk exposure in supplying that data to the AI tools they use. Sensitive information may be compromised if it is allowed to be ingested into an AI model. Pricing, product specifications and other vendor supplied data are typically subject to confidentiality restrictions that may be breached if used to train an AI model. Contracts that govern the supply of confidential information usually allow use of that information only for the purpose for which the data has been supplied, not the secondary use in model training. Further, the receiving party is normally required to return the confidential information upon the disclosing party's request, which becomes practically impossible if used to train an AI tool. Before implementing AI applications in the supply chain, companies should verify that all vendor data input into the tool can be used for training and retained for tuning and overfitting. Companies can attempt to negotiate terms that allow the use of de-identified and aggregated confidential information for training purposes, provided that the confidential information can no longer be recreated from the tool's output or traced to identify the disclosing party.

The issues with training data are not limited to questions of authorised use. The training process can incorporate biases present in the training data into the model, which can lead to outputs that perpetuate that bias and damage the decision-making processes. These biases can occur due to various factors, including historical data containing prejudices, lack of diverse representation in the data, and even the model developer's influence on the data collection process. When AI models are trained on biased data, those biases are reflected in the outputs and can have negative organisational and societal impacts. Recognising that biased algorithmic training data can lead to biased outcomes, New York City passed a first-in-the-nation law requiring employers that rely on algorithms to evaluate job applicants to have annual audits conducted by independent third parties to check for bias in outcomes, and to publish the results of those audits.[17] Biased outcomes can be detrimental to a company's reputation, due to unintentional discrimination from reliance on a biased AI model and can undercut a company's efforts to foster vendor diversity and inclusion. The effect of bias from algorithmic decision making led the Federal Trade Commission (FTC) to declare that the use of racially biased algorithms in AI-driven decision making is an unfair and deceptive business practice prohibited by the FTC Act and subjecting such matters to the general jurisdiction of the FTC.[18]

AI models improve through trial and error, effectively learning the desired actions to take in various circumstances as a result of the model's outcomes. This trial-and-error approach requires a considerable amount of computational

resources, and the learning process is frequently opaque, making the model's outcomes difficult to predict. In more complex models, the more accurate the outcome, the less explainable the model becomes (this is known as the accuracy-interpretability trade-off).[19] When algorithms are used to deny applications for credit or other adverse actions, however, the Consumer Financial Protection Bureau (CFPB) nonetheless requires that the company explains to applicants the specific reasons the action has been taken. In effect, such decisions must rely only on explainable AI.[20]

Opaque AI models can also lead to anomalous outcomes. Sometimes, the model generates outputs that are not based on actual data or factual information but are fabricated or distorted by the model itself. These spurious outputs are known as 'hallucinations' and can be quite detailed and difficult to detect. In 2023, a federal judge sanctioned two New York lawyers who used ChatGPT to research a brief submitted to the court.[21] When the opposing party notified the court that it was unable to find some of the cases cited in the other party's brief, it was discovered that the GenAI program had produced false citations, and judges' names and quotations from cases that did not exist. The court stated that there is nothing inherently wrong with using AI research tools, but that the lawyers have the gatekeeping obligation to vet the briefs before they are filed.

Fabricated results from AI models creates a trust issue and can strain relationships with vendors and customers. For instance, an AI system incorrectly predicting a surge in demand for a particular product can result in overstocking, increased carrying costs and potential obsolescence. Conversely, underestimating demand can result in stockouts, lost sales and damaged customer relationships. Human intervention and review is a necessary component of the responsible use of AI tools to prevent overreliance on automated outputs.

AI systems rely on connected networks to leverage big data and computational power to train and operate complex models. Data breaches can occur as a result of insufficiently secured databases or networks, which malicious actors can exploit to gain unauthorised access to sensitive information. Phishing schemes and other human engineering attacks target weak links in the supply chain, such as a smaller supplier with lesser security protocols, to make their way into larger companies' databases. Poorly secured application programming interfaces (APIs) can be exploited to extract data or introduce malicious code into the AI system.

LEGISLATION

The US has not enacted comprehensive legislation concerning the development and use of AI. In a political climate where bipartisan legislation is rare, there have been policy statements issued by the White House, and regulations issued by various federal agencies. In 2022, the White House released a policy paper entitled 'Blueprint for an AI Bill of Rights', setting out policy principles for regulation of AI.[22] The FTC issued guidance to businesses on unlawful discrimination due to bias in AI algorithms as well as a warning to marketers about exaggerating the results that AI-powered products can deliver.[23] The Food and Drug Administration (FDA) has issued guidance that some AI tools should be regulated as medical devices under the FDA's oversight of clinical decision support software.[24] There

is a patchwork of state laws directed at AI that have been recently enacted. Colorado passed a law requiring developers of high-risk AI systems to use reasonable care to avoid algorithmic discrimination.[25] Oregon updated its election law to require campaign communications that contain any synthetic media to include a disclosure that the content has been manipulated.[26] Utah enacted a consumer protection law requiring disclosure when using GenAI and limited the ability of businesses to avoid liability for consumer protection violations arising from use of AI.[27]

The European Union (EU), on the other hand, has enacted a sweeping omnibus law addressing the use of AI.[28] The EU AI Act classifies AI systems into four categories: unacceptable risk, high risk, limited risk and minimal risk. AI usage that is deceptive, certain facial recognition databases and biometric classification based on protected classes are all examples of prohibited uses. High-risk uses including recruitment and employment evaluation and financial and insurance determinations are required to be registered in a centralised database, have a quality management system and undergo compliance assessments. Limited risk applications, such as chatbots, are only subject to disclosure requirements, and minimal risk applications are unregulated. Because supply chains are frequently global in nature, organisations outside of the EU will need to evaluate AI tools they introduce into the supply chain for impacts on supply chain partners in the EU, and identify when the EU AI Act applies to them. Non-compliance carries significant penalties: administrative fines of up to €30m, and for companies, up to 6 per cent of their global annual turnover.

The contrast between the US and the EU on approaching the regulation of AI is similar to the approaches to the regulation of data privacy. At the federal level, the regulation of AI, like the regulation of data privacy, is at the sectoral level (eg healthcare, financial services). At the state level, there is some legislation, but it is typically targeted at specific behaviour. Only a few states have broader-based AI legislation. Data protection laws at the federal level have also been sectoral, such as the Gramm-Leach-Bliley Act (GLBA)[29] for financial data, and the Health Insurance Portability and Accountability Act (HIPAA)[30] for personal health information. In 2018, California enacted a sweeping data privacy law, the California Consumer Privacy Act of 2018 (CCPA),[31] that had much in common with the EU GDPR.[32] Since that time, nearly 20 other states have enacted broad ranging data privacy laws. In the absence of a federal AI law in the US, states may follow the same path and enact omnibus AI laws modelled on the EU AI Act.

CONCLUSIONS

AI has transformed supply chain data analysis, expanding the capabilities of managers to predict demand and formulate a comprehensive strategy for meeting that demand, including sourcing, production, distribution and customer service activities. But using AI solutions in supply chain and logistics is not without risk. The acquisition and use of training data for AI models needs to be rigorously examined for accuracy and quality, as well as for compliance and legal exposure. And the deployment of AI in the supply chain requires continuous monitoring and oversight.

Establishing an AI governance framework at the company level will give

the appropriate guidance to, and drive responsible use of, AI in supply chain management. The National Institute of Technology Standards (NIST) has published the Artificial Intelligence Risk Management Framework, which describes the life cycle of the responsible use of AI within an organisation. This framework addresses not only designers and developers of AI systems, but those who deploy and use AI in their organisations. Well-designed AI risk management frameworks should govern, map, measure and manage the AI life cycle in the organisation. These processes are intended to establish and maintain trustworthy AI systems, which are valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy enhanced and fair with their harmful biases managed. A robust AI risk framework is particularly important for supply chain management, where establishing trustworthy AI systems is especially difficult across geographically and organisationally diverse supply chain partners.

REFERENCES

(1) Subramanian, S. (March 2024), 'From 5MB Hard Drives To 180 Zettabytes: The Data Migration Challenge', *Forbes*, available at https://www.forbes.com/sites/forbestechcouncil/2024/03/04/from-5mb-hard-drives-to-180-zettabytes-the-data-migration-challenge/#:~:text=As%20of%202023%2C%20we%20cumulatively,reaching%20180%20zettabytes%20-by%202025 (accessed 9th August, 2024).

(2) Marr, B. (February 2024), '7 Ways Retailers Are Using Generative AI To Provide A Better Shopping Experience', *Forbes*, available at https://www.forbes.com/sites/bernardmarr/2024/02/29/7-ways-retailers-are-using-generative-ai-to-provide-a-better-shopping-experience/ (accessed 9th August, 2024).

(3) Bean, R. (January 2024), 'How Schneider Electric Is Deploying AI To Improve Energy Efficiency For All', *Forbes*, available at https://www.forbes.com/sites/randybean/2024/01/30/how-schneider-electric-is-deploying-ai-to-improve-energy-efficiency-for-all/#:~:text=Schneider%20Electric%20is%20applying%20AI,of%20sustainable%20solutions%20at%20scale. (accessed 9th August, 2024).

(4) Karim, S. (June 2024), 'How AI Can Lead to Personalized Medicine', Insurance Through Leadership, available at https://www.insurancethoughtleadership.com/life-health/how-ai-can-lead-personalized-medicine (accessed 9th August, 2024).

(5) Takyar, A., 'Generative AI in travel: Use cases, benefits and development', LeewayHertz, available at https://www.leewayhertz.com/generative-ai-in-travel/ (accessed 9th August, 2024).

(6) Dempsey, J. X. (August 2020), 'Artificial Intelligence: An Introduction to the Legal, Policy and Ethical Issues', p. 4, Berkeley Center for Law & Technology, available at https://imgsvr.edgereg.net/ERImg/02/91/24/LegalIssues-AI-April2019.pdf (accessed 9th August, 2024).

(7) Department of Justice (January 2023), 'Justice Department and Meta Platforms Inc. Reach Key Agreement as They Implement Groundbreaking Resolution to Address Discriminatory Delivery of Housing Advertisements', available at https://www.justice.gov/opa/pr/justice-department-and-meta-platforms-inc-reach-key-agreement-they-implement-groundbreaking (accessed 9th August, 2024).

(8) IBM, 'Generative AI in Supply Chain' available at https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/Generative-AI-supplychain (accessed 9th August, 2024).

(9) Richey Jr, R. G., Chowdhry, S., Davis-Srmaek, B. and Giannakis, M. (2023), 'Artificial intelligence in logistics and supply chain management: A primer and roadmap for research', *Journal of Business Logistics*, Vol. 44, No. 4, pp. 532–549.

(10) *Ibid*., p. 535.

(11) Pan, S. L. and Nishant, R. (October 2023), 'Artificial intelligence for digital sustainability: An insight into domain-specific research and future directions', *Journal of Information Management*, Vol. 72, 102668.

(12) *A.T., J.H. v. OpenAI LP et al*. Case No. 3:23-cv-04557 (N.D. Cal.) Filed 5th September, 2023.

(13) Browne, R. (April 2023), 'Italy became the first Western country to ban ChatGPT.

Here's what other countries are doing', CNBC, available at https://www.cnbc.com/2023/04/04/italy-has-banned-chatgpt-heres-what-other-countries-are-doing.html (accessed 9th August, 2024).
(14) *Zhang, et al. v. Google LLC, et al.*, Case No. 3:24-cv-02531 (N.D. Cal.) Filed 11th July, 2023.
(15) *Thomson Reuters Enterprise Centre GMBH et al. v. Ross Intelligence, Inc.*, Case No. 1:20-cv-613-SB (D. Del.) Filed 25th September, 2023.
(16) *Getty Images (U.S.), Inc. v. Stability AI, Ltd. et al.*, Case No. 1:23-cv-00135-GBW (D. Del.) Filed 29th March, 2023; *The New York Times Company v. Microsoft Corporation et al.*, Case No. 1:23-cv-11195 (S.D.N.Y.) Filed 27th December, 2023.
(17) New York City Local Law 144 of 2021.
(18) *Federal Trade Commission v. Rite Aid Corporation et al.*, Case No. 2:23-cv-05023 (E.D.P.A.) Filed 19th December, 2023.
(19) Hacker, P., Krestel, R., Grundmann, S. and Naumann, F. (2020), 'Explainable AI under contract and tort law: Legal incentives and technical challenges', *Artificial Intelligence and Law*, Vol. 28, pp. 415–439.
(20) Consumer Financial Protection Bureau (CFPB) (September 2023), 'CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence', available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-on-credit-denials-by-lenders-using-artificial-intelligence/ (accessed 9th August, 2024).
(21) *R. Mata v. Avianca, Inc.*, Opinion and Order on Sanctions. Case No. 1:22-cv-01461-PKC, 22nd June, 2023.
(22) The White House (2022), 'Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People', available at https://www.whitehouse.gov/ostp/ai-bill-of-rights/ (accessed 9th August, 2024).
(23) Federal Trade Commission (FTC) (February 2023), 'Keep Your AI Claims in Check', available at https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check (accessed 9th August, 2024).
(24) US Food & Drug Administration (US FDA) (May 2024), 'Artificial intelligence and machine learning (AI/ML)-enabled medical devices', available at https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices (accessed 9th August, 2024).
(25) Colorado General Assembly (2024), Col. Rev. Stat. §§6-1-1701 et. seq., 17th May, 2024, available at https://leg.colorado.gov/sites/default/files/documents/2024A/bills/2024a_205_enr.pdf (accessed 9th August, 2024).
(26) Oregon Legislative Assembly (March 2024), 'O. Rev. Stat. §260.345', available at https://web.archive.org/web/20240728162510/https://custom.statenet.com/public/resources.cgi?mode=show_text&id=ID:bill:OR2024000S1571&verid=OR2024000S1571_20240327_0_EF& (accessed 9th August, 2024).
(27) Justia US Law, 'Utah Code §13-2-2', available at https://law.justia.com/codes/utah/title-13/chapter-2/section-2/ (accessed 9th August, 2024).
(28) European Union (EU), 'Artificial Intelligence Act (March 2023), 'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828', available at https://eurlex.europa.eu/search.html?scope=EURLEX&text=AI+Act&lang=en&type=quick&qid=1722636836664 (accessed 9th August, 2024).
(29) Congress, 'Gramm-Leach-Bliley Act. 15 U.S.C. §§6801 et. seq., 12th November, 1999', available at https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm (accessed 9th August, 2024).
(30) Congress, 'Health Insurance Portability and Accountability Act of 1996. Pub. L. 104-191, 21st August, 1996', available at https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm (accessed 9th August, 2024).
(31) California Legislative Information, 'Cal. Civ. Code § 1798.185(a)(1)-(2), (4), (7). [4] § 1798.140(c), 3rd July, 2018', available at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (accessed 9th August, 2024).
(32) European Union (EU) (April 2016), '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, and repealing Directive 95/46/EC (General Data Protection Regulation)', available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (accessed 9th August, 2024).