



# AI Agents and Legal Intricacies: A Comprehensive Literature Review

Vikrant Sopan Yadav<sup>1\*</sup>  and Abhijeet Dhere<sup>2</sup> 

<sup>1</sup> Dr Vishwanath Karad MIT World Peace University, Pune, India  
vikrant.yadav@mitwpu.edu.in\*

<sup>2</sup> Dr Vishwanath Karad MIT World Peace University, Pune, India  
abhijeet.dhere@mitwpu.edu.in

**Abstract.** Artificial Intelligence agents have wide-scale applications in various sectors such as finance transportation, legal work, etc. Despite multiple benefits, these agents pose complex legal challenges. This paper performs a detailed examination of AI agent's legal complexity by analyzing liability, accountability, privacy requirements, intellectual property rights, and moral dilemmas. With the analytical method, this paper has synthesized scholarly research, case studies, and regulatory frameworks to gain a full appreciation of AI agents in legal matters. This effort of analyzing and consolidating the existing literature review, particularly concerning the legal intricacies revolving around the AI Agents provides the base for future research in the area of accountability and liability of the AI Agents. The current business environment experiences fundamental operational shifts because AI technology integration generates substantial consequences throughout multiple legal domains. From employment law to competition law, and from contract enforcement to consumer protection, the ripple effects of AI are felt everywhere. Legal discussion on AI involves critical analysis of several major issues, including liability questions, privacy protection matters, intellectual property rights concerns, and general ethical problems that exceed accepted social norms and legal principles. Each of these concerns is multi-layered, for example, liability debates touch on both civil and criminal law, while privacy and IP issues involve balancing innovation with individual rights. This has created a demand for immediate reorientation of the existing legal and regulatory framework. Without such reorientation, governments risk lagging behind technological development, leaving citizens and businesses exposed to uncertain and possibly harmful outcomes.

**Keywords:** AI Agent, Accountability, Liability, Regulations

## 1 Introduction

AI agents/applications (AIA) act as autonomous systems that demonstrate abilities to complete duties requiring human intelligence to perform them. Such systems become increasingly common. AI agents include basic chatbots and advanced autonomous vehicle systems as well as autonomous decision-making systems. The continuous progress of AI technology paves the way for legal challenges, which have become complex

© The Author(s) 2025

P. Sharma et al. (eds.), *Proceedings of the International Conference on Artificial Intelligence in Management for Business and Industrial Growth (AIMBIG 2025)*, Advances in Economics, Business and Management Research 355,

[https://doi.org/10.2991/978-94-6463-898-1\\_4](https://doi.org/10.2991/978-94-6463-898-1_4)

enough to require an immediate solution. Three critical issues – liability attribution, intellectual property (IP) disputes, and algorithmic bias; illustrate the tension between innovation and accountability. For instance, an autonomous Uber vehicle killed a pedestrian in Arizona in 2018, which led to uncertainty regarding accountability for damage by AIA. The National Transportation Safety Board (NTSB) identified the major reason of the accident to be defective safety measures, underlining the need for addressing the regulatory gaps in fixing responsibility on developers, operators, and/or users. Generative AI Company Stability AI faced major IP legal challenges after Getty Images sued the corporation in 2023 for infringing on their copyright by scraping millions of unapproved images (*Getty Images v. Stability AI*, 2025). Algorithmic bias is another legal challenge often faced by the world community. For instance, according to Angwin, J., et al. (2022), the COMPAS risk assessment tool identified African American defendants at higher rates for potential reoffending. Many AI systems operate as black boxes since developers often find it challenging to trace the decision-making processes. The exploitation of personal data without consent during AI-targeted advertising resulted in privacy violations as demonstrated in the Cambridge Analytica scandal of 2018.

In the case of generative AI agents, hallucination has been the biggest concern. In a high-profile case, attorneys Peter LoDuca and Steven A. Schwartz used ChatGPT to conduct legal research for a brief in *Mata v. Avianca, Inc.* (2023). The AI-generated brief included citations to six non-existent cases with fabricated quotes and judicial opinions. This led to a federal judge imposing a \$5,000 sanction on the attorneys. Similar instances were observed in *People v. Crabill* (2023).

The 2020 Belgian political party employed deepfake technology to create an incorrect video of a rival politician speaking divisive statements, which caused legal discussions about defamation during elections.

Different nations across the world pursue separate objectives through their regulatory frameworks. The European Union's AI Act (2021) introduced a system of risk classification, which led to the ban on intrusive technologies, including real-time biometric surveillance. The United States follows a sector-by-sector strategy that prioritizes ethical design although lacking enforceable rules. The United States is experiencing an escalating debate about Section 230 of the Communications Decency Act where lawmakers seek to make AI platforms responsible for harmful content that algorithms produce or spread. The Chinese government enforces transparency regulations for AI-driven content through the Algorithmic Recommendations Regulation, 2023 as part of its control over algorithmic manipulation determined by the Cyberspace Administration of China (Albrecht, D., 2022). Through its AI Ethics Recommendation (2021), UNESCO supports standardized ethical practices by asking member nations to prioritize human rights. The 2023 Interim Measures for Generative AI Services in China take a government-led method to manage AI outputs through national security rules while upholding public moral values. The distinct regulatory initiatives emphasize worldwide recognition of AI dangers yet demonstrate difficulties in standardization between authorities that maintain different economic and political goals, along with cultural backgrounds. Despite this progress, the legal system across the globe is still facing the uphill task of regulating the possible legal challenges arising from AIA.

## 2 Objectives of the study

This work aims to evaluate existing scholarly resources on AI agents and the legal challenges likely to result from their application of AIA. By synthesizing current literary resources, the study further aims to provide a foundation for future research on accountability and liability frameworks for AIAs.

## 3 Research Methodology

A thematic synthesis approach is adopted to investigate and classify the legal challenges arising from AI applications. Scherer (2016) argues that this design system enables the evaluation of different responsibility standards between product liability and negligence systems, as well as analyses of international IP rights frameworks. This systematic methodology ensures that the analysis remains coherent with the essential research tasks described in the paper's introduction section. Data was extracted from:

- Academic Databases: Google Scholar, IEEE Xplore, and PubMed for peer-reviewed articles (e.g., Buolamwini & Gebru, 2018).
- Legal Databases: LexisNexis and Westlaw for case law (e.g., Thaler v. Perlmutter, 2023).
- Regulatory Documents: EU AI Act (2024), GDPR (2018), and NIST Cybersecurity Framework (2020).

The research focused on studies released from 2015 to 2024 to reflect current legal developments. Key search terms used for the literature review include "AI liability," "privacy risks in AI," "AI-generated content ownership," and "algorithmic bias." The research excluded non-academic publications.

The authors organized literature content through four thematic classifications.

1. Liability: Examined frameworks for autonomous vehicles (Eykholt et al., 2018) and healthcare AI (Price et al., 2019).
2. The security of user data underwent an assessment regarding GDPR and data protection threats, according to Caliskan et al. (2017).
3. IP Rights: Compared jurisdictional stances on AI-generated content.
4. Mehrabi et al.'s (2021) evaluation of bias solution methods was investigated.

The research included multiple viewpoints by analyzing critiques concerning EU AI Act liability rules together with advocacy for human-centered intellectual property legislation. The research took steps to merge pro-innovation ideas and pro-regulation positions especially during debates on AI ethics. The study findings underwent cross-verification by peer discussions in iterative sessions and they matched the established research of Brundage et al. (2018) on malicious AI use and on regulatory strategies.

## 4 AI Agents and Legal Challenges

### 4.1 Liability

Determining liability is the primary legal issue that must be resolved when artificial intelligence systems inflict any sort of harm or damage to users. The current legal models that depend on human actions present challenges in determining liability when an AI system harms/damages someone.

According to, the scholarly recommendation of granting legal personhood to AI systems triggers substantial ethical and legal concerns. Giannini (2023) opined that AI technology demonstrates criminal behavior but cannot control itself, making it difficult to apply criminal laws to its activities. Identifying AI systems as human-operated tools creates clearer liability frameworks because developers and users would bear responsibility instead of the AI systems. Human responsibility presently appears to provide superior effectiveness in determining liability. Developers and users remain responsible for how they implement AI technologies. Therefore, legal frameworks should give priority to human accountability instead of assigning agency to AI systems.

Determining liability for damages by an AI agent requires examining fault-based liability through a rebuttable presumption of fault. Though strict liability applies to such situations, developers are granted specific protection if the agent's actions meet reasonable standards. The designer remains responsible for coding deficiencies even when analyzing curtailed autonomous decision-making systems from the AI agent.

Due to AI's opacity and unpredictability, proving causation requires establishing AI agent's liability. Victims find it hard to show evidence of defects or faults thus requiring new liability rules to simplify their proof obligations. Below is the comparative framework of AI agents' liability in different use cases.

**Table 1.** Comparative table of liability framework for varying acts/uses of AI Agent.

Type of AI Agent	Liability Framework	Responsible Parties	Key Considerations	Challenges
<b>Autonomous Vehicles</b>	Product liability, negligence, or strict liability depending on jurisdiction.	Manufacturers, software developers, or human operators (if override is possible).	Emphasis on "duty of care" and whether harm resulted from design flaws, algorithmic errors, or human misuse.	Complexity in attributing fault due to AI's autonomous decision-making.
<b>Healthcare AI</b>	Medical malpractice, product liability, or vicarious liability (hospital/institution).	Developers (if flawed design), healthcare providers (if misused AI)	Liability hinges on whether AI was used as a "tool" under professional oversight	Ambiguity in informed consent and transparency of AI-driven diagnoses.

		recommendations).	or as an autonomous decision-maker.	
<b>Customer Service Chat-bots</b>	Contractual liability, consumer protection laws, or negligence.	Service providers, developers (if biased/misleading outputs).	Focus on compliance with consumer rights (e.g., GDPR for EU users) and accuracy of information provided.	Proving causation between AI error and financial/emotional harm.
<b>Financial AI</b>	Regulatory compliance (e.g., SEC, MiFID II), negligence, or breach of fiduciary duty.	Financial institutions, algorithmic traders, or auditors.	Liability for market manipulation, biased lending, or erroneous trading decisions. Strict documentation requirements for explainability.	Black-box algorithms complicate accountability; regulatory fragmentation.
<b>Military AI</b>	International humanitarian law (IHL), state responsibility, or command accountability.	State actors, military commanders, or manufacturers (if violating IHL principles).	Compliance with proportionality and distinction in warfare. Human oversight required for lethal decisions ("meaningful human control").	Attribution challenges in cyber warfare; lack of global consensus on autonomous weapons.

<b>Content Moderation AI</b>	Intermediary liability (Section 230 in the US), defamation, or human rights violations.	Platform operators (if negligent in addressing harmful content).	Balancing free speech with harm prevention. Platforms may avoid liability if acting in "good faith" to remove illegal content.	Over-censorship or under-enforcement due to algorithmic bias; jurisdictional conflicts.
------------------------------	---	--	--	---

**Product Liability.** Under product liability law, a manufacturer remains responsible for any defects found in their products. The laws become difficult to apply to autonomous AI systems because of their self-driven operation. It is still difficult to answer the question of liability in cases such as accidents caused by autonomous vehicles. The current legal liability systems lack sufficient methods to handle the emotional distress and discrimination problems AI technology brings.

In reforming the liability framework, the US FDA's medical device regulations can form the basis for an adaptive product liability system that supports AI technology development (Sharkey, 2024). According to Lee (2024), a risk-based liability model should be implemented to handle the intricate nature of AI technologies because this approach suits pharmaceutical industries that employ generative AI systems.

In the EU, the proposed AIA will introduce new risk-management procedures to supervise AI systems focusing on both consumer security and responsibility issues. Under the AIA's provisions, providers who offer high-risk AI systems maintain complete legal responsibility when their products cause damages, especially when decision-making biases or safety-critical failures emerge in healthcare diagnostics and autonomous vehicle applications (European Commission, 2021). The new legal standard establishes different product responsibility standards since it addresses AI systems' obscurity through transparency requirements, audit tracking systems, and risk management protocols. Opponents of the AIA accuse the liability standards of creating unreasonable financial hardship for small businesses, yet supporters view its potential to improve ethical AI development and resolve AI-driven systematic negative effects (Wachter et al., 2021). The regulation supports EU-wide initiatives, including the 2023 revised Product Liability Directive that extends product fault liability to software defects and system malfunctions even when claimants do not need to prove vendor negligence (European Parliament, 2023).

### Summary:

- Product liability law holds manufacturers accountable for product defects.
- Applying these laws to autonomous AI is difficult due to AI's self-driven operations.
- Liability for accidents caused by autonomous vehicles remains unresolved
- Current legal systems inadequately address AI-related emotional distress and discrimination.

- The US FDA's medical device regulations could inspire adaptive AI product liability frameworks.
- A risk-based liability model is suggested for AI, similar to models in pharmaceuticals.
- The EU's proposed Artificial Intelligence Act (AIA) introduces risk-management procedures for AI oversight.
- Under the AIA, providers of high-risk AI systems bear full legal responsibility for damages.
- The AIA mandates transparency, audit tracking, and risk management to handle AI system opacity.
- Critics argue the AIA imposes financial burdens on small firms, while supporters see ethical benefits.
- The EU's revised 2023 Product Liability Directive extends liability to software defects without requiring proof of negligence.

**Negligence.** Negligence in AI's actions leads to additional problems that need attention. When an AI system produces substandard results, what entity accepts accountability, the user, the developer, or the AI itself? According to Selbst, A. D., (2020), the present legal framework provides no definite standards concerning this matter. Self-learning algorithms complicate the question of liability due to their advanced systems, making it challenging to attribute blame because developers cannot identify whether it was the AI's actions or the users' actions that led to the system's decisions. Developer and programmer liability stems from guilt-based principles, but the principle of risk applies to producer and user responsibility (Widło, 2024). Again, compliance with strict liability rules for dangerous AI applications would simplify reimbursement processes because it requires a determination of cause relationships rather than fault-based determination.

Some scholars (Fotheringham & Smith, 2024) argue for a second opinion to establish AI's liability; thus, healthcare professionals bear full responsibility even when jointly making decisions, while these ambiguities require legal reforms. A healthy debate exists about how AI displays 'quality of will,' which implies that blame attribution toward AI could become possible (Altehenger et al., 2024). Lawmakers still face major difficulties when pursuing liability for negligence against AI systems under present laws, but active discussions seek better moral and juridical approaches to resolve these issues efficiently.

### **Summary:**

- Negligence in AI raises accountability issues, whether responsibility lies with the user, developer, or the AI itself.
- Self-learning algorithms complicate liability attribution since their decisions blur developer and user responsibility.
- Liability frameworks distinguish between guilt-based responsibility for developers and risk-based responsibility for producers/users.
- Strict liability for dangerous AI applications could simplify reimbursement by focusing on causation rather than fault.

- In healthcare, some scholars argue professionals should bear full responsibility even when decisions are shared with AI.
- Ongoing debates include AI's potential "quality of will" and the need for legal reforms, as current laws struggle to address negligence in AI systems.

## 4.2 Privacy

AI agents need large quantities of information to operate effectively. However, this drives a major privacy problem that demands attention to consent, the need for transparent practices, and the risks of surveillance misuse.

The GDPR principles, help maintain an optimal relationship between creative thinking and privacy protection. India, among other countries, is implementing the Personal Data Protection Bill to manage the privacy challenges that AI generates (Karthikeyan, 2024). Researchers advocate for creating a data-conscious society and gaining control over their personal information to effectively protect their privacy.

**Data Collection and Consent.** Every individual needs to be fully informed about how their data will be used, especially in cases of sensitive healthcare information. People need to understand how their data will be used because clear data usage explanations build trust while providing them with the information required to make educated decisions about participating in research or other activities. The development of both explainable AI systems and dynamic consent systems serves to make data purposes transparent to patients regarding their healthcare data usage and computational choices. (Al-balawi et al., 2024).

All data collection and utilization practices by AI agents need to comply with privacy laws, such as the GDPR of the European Union. Safdar, N. M., et al. (2020) observe that technological agents face issues from data collection without permission and unintended data application.

To hold AI developers accountable and achieve fair results, developers should demonstrate full transparency in their process implementations.

**Data Security.** Organizations can detect system anomalies with the help of real-time predictive analytics, resulting in response durations of less than 1.5 minutes. Integrated automated response solutions increase operational performance by enabling organizations to resolve their security issues without delay (Weng & Wu, 2024).

Though AI may help ensure security, it poses severe security challenges. Protecting the safety of data that AI agents obtain stands out as a vital security matter. The development of explainable AI frameworks becomes essential because algorithmic biases and adversarial attacks make AI models vulnerable to attacks, thus requiring transparency. The security vulnerability of data through targeted attacks results in both unauthorized access and corrupted information (Ilieva & Stoilova, 2024). Scholars like Devineni, S. K. (2024) identifies the severe impacts of data breaches that include identity theft coupled with financial losses. The analysis by Kolade et al. (2024) discovered

that breaches caused by AI systems receive high regulatory points, which stresses the importance of developing strong governance frameworks.

AIA systems integrated into the healthcare and finance sectors are at risk of data breaches and unauthorized access. These systems must address significant privacy issues because they process extensive amounts of sensitive information, thus creating more (Brundage et al., 2018).

The General Data Protection Regulation (GDPR) and the EU Artificial Intelligence Act impose additional complexity on organizations by compelling them to establish secure measures that combine encryption and access controls to preserve AI operation transparency (European Commission, 2021). The National Institute of Standards and Technology [NIST] (2020) points out that organizations need to proactively take measures, including security audits along with sticking to the NIST cyber security framework to reduce security risks. Data security depends on resolving multiple challenges to utilize AIA functionality properly.

Summary:

- AI systems require vast amounts of data to function effectively.
- This dependence creates significant privacy risks, including surveillance misuse.
- Global and national regulations (e.g., GDPR, data protection laws) aim to safeguard personal privacy.
- Building a society that is aware of data rights helps individuals protect their information.
- Consent is a cornerstone of ethical AI data use.
- Individuals must be clearly informed about how their data is collected and applied.
- Transparent explanations of data use build public trust.
- Explainable AI systems improve clarity around how decisions are made with data.
- Dynamic consent systems give individuals more control over how their data is re-used.
- Developers need to follow privacy laws rigorously in all data practices.
- Transparency in developer processes is necessary for accountability and fairness.
- AI can support security by enabling rapid anomaly detection and automated responses.
- However, AI systems are also vulnerable to attacks such as adversarial manipulation and data corruption.
- Data breaches linked to AI can cause identity theft, financial losses, and reputational harm.
- Robust governance frameworks, encryption, access control, and regular audits are vital to managing AI privacy and security risks, especially in sensitive fields like healthcare and finance.

### 4.3 Intellectual Property Rights

Intellectual property rights remain contentious when artificial intelligence agents are developed or operated. AI-generated content ownership creates problems especially

when analyzing the datasets AI models use for training purposes. The lawsuit Getty Images, INC. v. Stability AI, INC. showcases the debate between parties regarding ownership of content and copyright violations.

**Ownership of AI-Generated Content:** The ambiguity of today's IP regulations allows disputes to arise on questions such as, are there any rights to the outputs produced by an AI agent that belongs to its owner? Does the AI itself own its intellectual property, or does it belong to the developers who made the AI agents or the consumers who use them? The legal ownership of datasets used for AI model training determines the ownership of generated content, producing complex legal conflicts between authors and AI tech firms. China and other copyright regimes have added new open-ended rules that intend to manage AI-generated work yet encounter classification and originality problems (He & Shan, 2024).

**Table 2.** Judicial reflection on legal ownership of AI-generated content

Jurisdiction	Legal Position	Reference	Key Provision/Excerpt
<b>United States</b>	No copyright protection for purely AI-generated works; requires human authorship.	<i>Copyright Act (17 U.S.C. § 102(a)); Thaler v. Perlmutter (D.D.C. 2023)</i>	"Copyright protection subsists in original works of authorship fixed in any tangible medium of expression, created by a human author." (17 U.S.C. § 102(a))
<b>European Union</b>	Only human-authored works qualify for copyright. AI output is unprotected.	<i>EU Copyright Directive (2019/790); Infopaq International A/S v. Danske Dagblades Forening (CJEU, 2009)</i>	"The author of a work shall be the natural person who creates it." (Art. 2(1), Copyright Directive)
<b>United Kingdom</b>	Copyright vests in the person arranging the creation of computer-generated works.	<i>Copyright, Designs and Patents Act 1988 (CDPA), Section 9(3); Nova Productions v. Mazooma Games (2007)</i>	"In the case of a computer-generated work, the author shall be the person by whom the arrangements necessary for the creation are undertaken." (CDPA §9(3))
<b>Japan</b>	Copyright may apply if human creativity is involved in AI output.	<i>Japanese Copyright Act (Art. 2(1)); Agency for Cultural Affairs Guidelines (2021)</i>	"A work must be a production in which thoughts or sentiments are creatively expressed by a human." (Art. 2(1))

<b>China</b>	Copyright requires human creation; AI works lack explicit protection.	<i>Copyright Law of China (2020 Revision)</i> , Art. 3; <i>Tencent v. Yinxiang</i> (Shenzhen Court, 2019)	"Works protected by copyright must be intellectual achievements with originality created by humans." (Art. 3)
<b>Australia</b>	No copyright for AI-generated works; human authorship required.	<i>Copyright Act 1968 (Cth)</i> , Section 32(4); <i>Commissioner of Patents v. Thaler</i> (2022)	"Copyright is personal property and subsists in original works originating from a human author." (Sec. 32(4))

**Patentability of AI Inventions.** A major challenge emerges when addressing whether AI agents can qualify to receive patent approvals for their inventions. AI systems can gain inventor status according to legal definitions. Several recent court decisions have denied such patents yet the subject remains contested (Sharma, S., & Pandey, D. 2022). Scholars (Ballardini et al., 2019) observe that, under existing patent frameworks, a human inventor must exist. AI-generated inventions face problems because they often lack human involvement, either minimal or absent.

Patentability policies suffer from a lack of uniformity across the globe. India disallows patents for software and algorithms, yet the United Kingdom and the United States grant software patents to those who demonstrate technical effects. The uniqueness of AI requires nations to develop standardized patent laws.

**Table 3.** Intellectual Property Rights (IPR) challenges in AIA inventions

<b>IPR Aspect</b>	<b>Challenge in AIA inventions</b>	<b>Example</b>	<b>Reference</b>
<b>Patents</b>	Determining inventorship when AI systems autonomously generate novel innovations.	AI-generated drug formulas without clear human inventor attribution.	(World Intellectual Property Organization [WIPO], 2021)
<b>Copyright</b>	Authorship disputes over AI-generated content (e.g., text, art, music).	AI-created artworks or articles lacking a human "author" under current law.	(United States Patent and Trademark Office [USPTO], 2020)
<b>Trade Secrets</b>	Protecting proprietary AI algorithms while complying with transparency requirements.	Balancing secrecy of AI training data with regulatory scrutiny.	(European Union Agency for Cybersecurity [ENISA], 2022)

<b>Data Ownership</b>	Ambiguity in ownership rights over datasets used to train AI models.	Disputes over rights to medical data used in AI-driven diagnostics.	(UK Intellectual Property Office [UK IPO], 2020)
<b>Ethical IPR Issues</b>	Balancing IP protection with societal access to AI innovations (e.g., healthcare).	Patenting AI-driven diagnostic tools limiting affordability in developing nations.	(Brundage et al., 2018)

The ability of Generative AI to spread content creation opportunities faces a major challenge against the loss of creative work quality and financial stability for professional creators. According to experts who advocate for protecting human creators' rights, IPR models need revisions. The music industry demands both open disclosure and reasonable payment systems for creators since AI technologies demonstrate exceptional influence in this field.

#### 4.4 Ethical Considerations

The domain of privacy protection must resolve various ethical matters that encompass data security, unbiased algorithmic values, checks on authority, and determining equilibrium between technological development and ethical standards. Some of these ethical challenges are discussed below.

**Bias and Discrimination.** AI systems reproduce the biases they receive in training data or algorithms and generate discriminatory results. According to Buolamwini & Gebru (2018), facial recognition systems generated more errors when analyzing photos of women and people with darker skin tones. The deployment of AI systems faces the challenge of equal treatment and fair practices (Ferrer, X., et al., 2021).

According to Bueno (2024), deployment of AI systems, which inherit bias from their training data because of discriminatory input, results in worsening existing social inequalities with a particular impact on women and disadvantaged minorities. The AI development team needs to make fairness-aware algorithms an implementation priority while using datasets that contain diversity (Mehrabi et al., 2021). XAI (explainable AI) is essential, for providing transparent monitoring in vital areas, including criminal justice and medical diagnosis. Under the EU's General Data Protection Regulation (GDPR), there exists a requirement to provide explanations for automated decisions, which organizations must fulfill. The IEEE's Ethically Aligned Design and other ethical guidelines defend human oversight within AI decision-making systems.

**Autonomy and Control.** The increasing autonomy of AI agents challenges traditional notions of control and responsibility. The ethical challenges of AI and autonomous systems include ensuring safety, transparency, and accountability while prioritizing human

values. According to scholars, the question of how much autonomy AI agents should have and who should oversee their actions needs attention.

### 5 Findings

An extensive literary analysis shows that various AI applications have varying risk probability to privacy. The table below shows the literature studied in the present works, which throws light on the level of risks associated with different AI applications.

**Table 4.** Privacy Risks Across AI Applications (Generated with python using matplotlib and pandas)

AI Application	Severity Score	Frequency	Risk Level	Reference
Membership Inference Attacks	2.75	>3x	High	(Eykholt et al., 2018; Caliskan et al., 2017; Fredrikson et al., 2015; Goodfellow et al., 2014)
Healthcare Diagnostics	2.40	2x	Moderate	
Autonomous Vehicles	2.20	1x	Moderate	
Social Media Algorithms	2.10	1x	Moderate	
Retail Personalization	1.80	1x	Moderate	
Language Processing (NLP)	1.35	<1x	Low	
Image Recognition	1.00	<1x	Low	

Risk Score Key: High (>2.5) | Moderate (1.5–2.5) | Low (<1.5)

Risk Distribution by Category

Total Identified Risks: 100%

- High-Risk Applications: 15% (Membership Inference Attacks)
- Moderate-Risk Applications: 60% (Healthcare, Autonomous Vehicles, Social Media, Retail)
- Low-Risk Applications: 25% (NLP, Image Recognition)

A table organizes privacy risks across AI applications, displaying severity levels together with their frequency of occurrence, supported by research citations. Table 4 shows membership inference attacks rated at 2.73 and image recognition rated at 1.00 presents the primary concern. The evaluation combines risk severity with recurrence rates, which represent identified frequencies of real-world risk occurrences.

Table 4 depends on actual research studies to produce quantitative data about AI privacy risks.

- Membership Inference Attacks receive a score of 2.73 since they successfully reveal training data thus earning the highest ranking.
- Healthcare Diagnostics risks stem from sensitive patient data exposure.
- According to Eykholt et al. (2018) autonomous vehicles encounter disruptive sensor data attacks that endanger their performance.
- Social Media Algorithms (Caliskan et al., 2017) contain intentional and unintentional biases because of their revealed data leakage.
- The Retail Personalization sector encounters GDPR (2018) compliance difficulties when performing consumer profiling.
- Implementing differential privacy reduces security risks for Language Processing (Fredrikson et al., 2015) and Image Recognition (Goodfellow et al., 2014).

The literature survey on Google Scholar revealed legal risks from AI Agents and applications, which are listed below in a table.

**Table 5.** Literature survey on legal issues associated with AIA

<b>Legal Issue</b>	<b>Source/Reference</b>
Product Liability	Borges, G., 2022
Negligence	Selbst, A. D., 2020
Data Collection and Consent	Safdar, N. M., et al., (2020); Alqodsi, E. M., et al., 2024
Data Security	Devineni, S. K. 2024
Ownership of AI-Generated Content	Kirakosyan, A., 2023
Patentability of AI Inventions	Sharma, S., & Pandey, D., 2022
Bias and Discrimination	Ferrer, X., et. al., 2021; Hanna
Autonomy and Control	Riva, G., & Tiribelli, S. (2022)

## 6 Conclusion

Artificial intelligence (AI) systems in commercial industries create complex legal problems that need immediate attention from lawmakers and non-state actors. These problems are not confined to isolated incidents; instead, they cut across sectors, raising profound questions of accountability, transparency, and fairness that cannot be ignored. The current business environment experiences fundamental operational shifts because AI technology integration generates substantial consequences throughout multiple legal domains. From employment law to competition law, and from contract enforcement to consumer protection, the ripple effects of AI are felt everywhere. Legal discussion on AI involves critical analysis of several major issues, including liability questions, privacy protection matters, intellectual property rights concerns, and general ethical problems that exceed accepted social norms and legal principles. Each of these concerns is multi-layered, for example, liability debates touch on both civil and criminal law, while

privacy and IP issues involve balancing innovation with individual rights. This has created a demand for immediate reorientation of the existing legal and regulatory framework. Without such reorientation, governments risk lagging behind technological development, leaving citizens and businesses exposed to uncertain and possibly harmful outcomes.

The advancing speed of AI technology aligns with the findings from the aforementioned references and data, necessitating a transformation in existing legal structures so businesses can harness AI's strengths while managing its potential negative outcomes. This transformation is not simply optional; it has become an unavoidable strategic requirement for sustainable growth. This, of course, will help citizens as well. If managed carefully, reformed systems will not only protect individuals from harm but also ensure equitable distribution of AI's benefits. Faster AI innovation presents unexpected circumstances that require legislators to develop proactive solutions instead of waiting for problems to emerge. Waiting until after damage occurs would only deepen social, financial, and ethical crises, potentially eroding trust in both technology and governance. The existing data suggests that this step needs to be taken as soon as possible, as the challenges posed by the gaps in policy and regulation can result in major issues. Among these issues are risks of unchecked monopolies, discriminatory outcomes, breaches of sensitive data, and systemic failures in safety-critical industries such as healthcare and transportation.

Research within science should concentrate on creating complete regulatory systems to handle these complicated matters effectively. Such research should not be limited to theoretical debate but must also produce practical guidelines, models, and benchmarks that regulators and industries can apply in real-world contexts. Scientific research should create detailed policies to determine responsible AI use, followed by data security protocols that guarantee maximum protection for individual information. These policies must be flexible enough to adapt to future innovations while still offering robust safeguards against foreseeable risks. The creation of technology-friendly ethical standards requires immediate collaboration between technologists, legal professionals, and ethicists. This collaborative spirit should be institutionalized through cross-disciplinary councils, public consultations, and ongoing international dialogue, ensuring that ethical standards remain dynamic and inclusive. The effort is essential since it defends all stakeholders and creates responsible and ethical conditions where innovative work can flourish, leading to a healthier and more equitable society during rapid technological advancement. Ultimately, the future of AI will depend not only on the brilliance of its technological breakthroughs but also on the wisdom of the legal and ethical frameworks designed to guide its use.

## References

1. Albalawi, A. F., Yassen, M. H., Almuraydhi, K. M., Althobaiti, A. D., Alzahrani, H. H., & Alqahtani, K. M. (2024). Ethical Obligations and Patient Consent in the Integration of Artificial Intelligence in Clinical Decision-Making. *Journal of Healthcare Sciences*, 04(12), 957–963.

2. Albrecht, D. (2022). The Internet Information Services Algorithm Recommendation Management (IISARM) Regulations in China. *Computer Law Review International*, 23(4), 97-103.
3. Alqodsi, E. M., Jadalhaq, I. M., El Maknouzi, M. E. H., & Abdulhay, I. E. A. (2024). Navigating the Legal Landscape: AI Adoption in Education and Teacher Responsibilities. In *Cutting-Edge Innovations in Teaching, Leadership, Technology, and Assessment* (pp. 212-230). IGI Global.
4. Altehenger, H., Menges, L., & Schulte, P. (2024). How AI Systems Can Be Blameworthy. *Philosophia*.
5. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2022). Machine bias. In *Ethics of data and analytics* (pp. 254-264). Auerbach Publications.
6. Ballardini, R. M., He, K., & Roos, T. (2019). AI-generated content: authorship and inventorship in the age of artificial intelligence. In *Online Distribution of Content in the EU* (pp. 117-135). Edward Elgar Publishing.
7. Bonilla Gutiérrez, J. C. (2024). IA y Privacidad: Protegiendo la Autodeterminación Informativa en la Era Digital. *Revista de La Facultad de Derecho de México*, 74(290), 125-148.
8. Borges, G. (2022). Liability for autonomous systems. In *Law and Technology in a Global Digital Society: Autonomous Systems, Big Data, IT Security and Legal Tech* (pp. 51-73). Cham: Springer International Publishing.
9. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint*, arXiv:1802.07228.
10. Bueno, D. J. (2024). Gender bias in artificial intelligence: a critical perspective and legal analysis. *Amicus Curiae.*, 26, 20-29.
11. Buolamwini, J., & Gebru, T. (2018, January). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency* (pp. 77-91).
12. Caliskan, A., Bryson, J. J., & Narayanan, A. (2017). Semantics derived automatically from language corpora contain human-like biases. *Science*, 356(6334), 183-186.
13. Chatterjee, S., Mohanta, A., & Sneha, S. (2024). Navigating AI Liability in Criminal Law. *Advances in Finance, Accounting, and Economics Book Series*, 311-334.
14. Devineni, S. K. (2024). AI-enhanced data visualization: Transforming complex data into actionable insights. *Journal of Technology and Systems*, 6(3), 52-77.
15. Eykholt, K., et al. (2018). Robust physical-world attacks on deep learning visual classification. *IEEE CVPR*, 1625-1634. <https://doi.org/10.1109/CVPR.2018.00175>
16. Ferrer, X., Van Nuenen, T., Such, J. M., Coté, M., & Criado, N. (2021). Bias and discrimination in AI: a cross-disciplinary perspective. *IEEE Technology and Society Magazine*, 40(2), 72-80. DOI:10.1109/MTS.2021.3056293
17. Fotheringham, K., & Smith, H. (2024). Accidental injustice: Healthcare AI legal responsibility must be prospectively planned prior to its adoption. *Future Healthcare Journal*, 11(3),
18. Fredrikson, M., Jha, S., & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures. *ACM SIGSAC*, 1322-1333.
19. *Getty Images v. Stability AI*. [2025] EWHC 38
20. Giannini, A. (2023). Criminal behavior and accountability of artificial intelligence systems.
21. Gilbert, C., & Gilbert, M. A. (2024). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. *International Journal of Scientific Research and Modern Technology*, 9-17.

22. Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. *arXiv:1412.6572*.
23. He, X., & Shan, P. (2024). China's regulations on the attribution of AI-generated content: an exploration based on the open-ended approach. *Journal of Intellectual Property Law & Practice*.
24. Ilieva, R., & Stoilova, G. (2024, September). Challenges of AI-Driven Cybersecurity. In *2024 XXXIII International Scientific Conference Electronics (ET)* (pp. 1-4). IEEE.
25. *Infopaq International A/S v. Danske DagbladesForening*, Case C-5/08. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62008CJ0005>
26. Karthikeyan, C. (2024). AI (Artificial Intelligence) Integration for Integrity Ethics and Privacy in AI-Driven Organizations. *Advances in Business Strategy and Competitive Advantage Book Series*, 51–76.
27. Kazimi, J., & Thalwal, H. (2024, June). Intellectual Property Protection in AI-driven Innovations: A Comparative Analysis. In *2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP)* (pp. 320-326). IEEE.
28. Kirakosyan, A. (2023). Intellectual property ownership of AI-generated content. *Digital LJ*, 4, 40.
29. Kolade, T. M. (2024). Artificial Intelligence and global security: Strengthening international cooperation and diplomatic relations. *Available at SSRN 4998408*.
30. Lee, S. (2024). A study on civil liability of Artificial Intelligence. *MinsaBeob'hag*, 107, 225–261.
31. Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM computing surveys (CSUR)*, 54(6), 1-35.
32. Riva, G., & Tiribelli, S. (2022). Moral and legal autonomy in the era of artificial intelligence. *S&F SCIENZA E FILOSOFIA. IT.*, 28, 166-202.
33. Safdar, N. M., Banja, J. D., & Meltzer, C. C. (2020). Ethical considerations in artificial intelligence. *European journal of radiology*, 122, 108768.
34. Scherer, M. U. (2015). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harv. JL & Tech.*, 29, 353.
35. Selbst, A. D. (2020). Negligence and AI's human users. *BUL Rev.*, 100, 1315.
36. Sharkey, C. M. (2024). A Products Liability Framework for AI. *Columbia Science and Technology Law Review*, 25(2).
37. Shahriari, K., & Shahriari, M. (2017, July). IEEE standard review—Ethically aligned design: A vision for prioritizing human wellbeing with artificial intelligence and autonomous systems. In *2017 IEEE Canada international humanitarian technology conference (IHTC)* (pp. 197-201). IEEE.
38. Sharma, S., & Pandey, D. (2022). The Use of AI in Patent Law: Issues and Challenges. *Issue 5 Indian JL & Legal Rsch.*, 4, 1.
39. *Thaler v. Perlmutter*, No. 22-CV-384-1564-BAH. <https://www.wipo.int/wipolex/en/judgments/details/1840>
40. Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, 41, 105567.
41. Weng, Y., & Wu, J. (2024). Leveraging Artificial Intelligence to Enhance Data Security and Combat Cyber Attacks. *Deleted Journal*, 5(1), 392–399.
42. Widło, J. (2024). Tortious Liability for Using Artificial Intelligence. *Teka Komisji Prawniczej PAN Oddział w Lublinie/Teka Komisji Prawniczej*, 17(2), 529–545.

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

