THE American Journal of Humanities and Social Sciences Research (THE AJHSSR) 2026
E-ISSN: 2581-8868
Volume-09, Issue-04, pp-48-73
www.theajhssr.com Crossref DOI: https://doi.org/10.56805/ajhssr
Research Paper Open Access

The Future and Challenges of Artificial Intelligence Law: Perspectives of Economy, Technology Industry, Culture, Human Behavior and Fraud

Jyh-Woei Lin
Department of Electrical Engineering, Southern Taiwan University of Science and Technology, Tainan, 710301, Taiwan, Tel: +886(0) 966132209,
https://orcid.org/0000-0001-6875-0172

ABSTRACT

The rapid development of artificial intelligence (AI) is profoundly impacting society, the economy, ethics, and legal systems. AI applications extend from industrial automation, medical diagnosis, and financial investment to traffic management, judicial assistance, and the creative industries, posing unprecedented challenges to the existing legal framework. This article delves into the core issues of AI law, focusing on liability definition, data protection, intellectual property rights, algorithmic transparency and international coordination. It analyzes future development trends and major challenges, and proposes feasible policy recommendations and legal response strategies. The research results indicate that AI law needs to balance technological innovation, ethical responsibility, and social security, and should strengthen international cooperation to establish a forward-looking, resilient, and cross domain coordinated legal governance framework. In addition, we focus on the impacts of AI law on economy, technology industry and culture, as well as the relationships between AI law and human behavior, and between fraud and AI law.

KEYWORDS: Artificial Intelligence (AI); Core Issues of AI Law; Technological Innovation; Ethical Responsibility; Social Security

* Corresponding Author: Jyh-Woei Lin

1. INTRODUCTION

Artificial intelligence (AI) technology **(Figure.1)** has experienced explosive growth in the past decade, particularly the rise of generative AI **(Figure.2)** (Batty, 2025; Van Quaquebeke et al., 2025**)**, deep learning and automated decision-making systems (Ahsen et al., 2025), which have had a profound impact on social governance, industrial development, and legal systems (Vivo, et al., 2025). Legal systems are structured frameworks of rules, institutions, and procedures used by societies to interpret, enforce, and create laws. They maintain social order, resolve disputes, and protect rights, predominantly classified into four main types, common law, civil law, religious law and customary law or combinations thereof. Automated decision-making

systems (Lukács and Váradi, 2023; Boos, 2024; Miah et al., 2026) are computer based tools, including AI-driven software, that analyze vast datasets to help users select the optimal course of action among alternatives. They enhance efficiency in areas like supply chain management and predictive maintenance, transitioning from automated, rule-based processes to intelligent systems that learn and adapt to complex scenarios. AI has not only improved productivity and decision-making accuracy but has also deeply influenced daily life. For example, autonomous vehicles (Yang et al., 2025) can reduce traffic accident rates, but the legal responsibility for accidents remains unclear. Autonomous vehicles, also known as self-driving or driverless cars, use sensors, software, and AI to navigate and operate with little to no human intervention. While fully autonomous personal vehicles are not yet available for purchase, major cities in the U.S. and China already host commercial robotaxi fleets. Medical AI systems (Akila et al., 2025) can assist in diagnosing diseases, but if misdiagnosis leads to patient harm, current laws cannot clearly define the responsible party. Medical AI systems leverage machine learning, deep learning and natural language processing to revolutionize healthcare, with 77% of U.S . The U.S. Food and Drug Administration (FDA) already approved AI devices as of 2025 focusing on radiology. The U.S. FDA encourages the development of innovative, safe, and effective medical devices, including devices that incorporate AI. Some main applications include enhancing diagnostic accuracy (e.g., detecting cancers or retinal diseases), automating administrative tasks, drug discovery, and personalized treatment planning. These above phenomena highlight the gap between current legal systems and the development of AI technology. The development of AI technology is profoundly transforming legal systems worldwide, shifting from speculative, future-oriented debates to practical, everyday integration, particularly through tools for legal research, document automation, and judicial case management. As AI adoption grows, it faces critical challenges regarding ethical biases, black box algorithms (Chen et al., 2024), data privacy, and accountability, necessitating, as of 2025-2026, a surge in regulatory, ethical and legislative frameworks (e.g., the European Union (EU) AI Act) to ensure these technologies align with principles of justice, transparency, and the rule of law.

As of 2025–2026, the proliferation of black box AI algorithms, systems whose decision-making processes are too complex for humans to interpret, has created an urgent, global surge in regulatory, ethical, and legislative frameworks aimed at ensuring data privacy and accountability. The core challenge is that opaque models can perpetuate biases and operate without transparency, necessitating a shift from testing to "enforcement of AI governance in high stakes sectors like finance, healthcare, and cybersecurity. Following its adoption, the EU AI Act's governance rules and obligations for General Purpose AI (GPAI) models became active in August 2025, with strict, risk based transparency requirements for high risk systems. High-risk systems, defined under the EU AI Act, are AI applications posing significant risks to health, safety, or fundamental rights. They include AI in critical infrastructure, education, employment, biometric identification, and law enforcement. These systems require strict compliance, including risk management, high-quality data, technical documentation, and human oversight. The GPAI models are versatile, large-scale AI models (e.g., GPT-4) trained on vast data that perform diverse tasks, from image recognition to content generation (Triguero et al., 2024). Under the EU AI Act, they are regulated based on capabilities and potential systemic risks. Key obligations for providers include

maintaining technical documentation, upholding copyright policies, and publishing training summaries. 2026 is marked by the activation of comprehensive state laws, such as the Colorado AI Act (effective June 2026), the Colorado AI Act is a first-of-its-kind state law in the U.S. designed to protect consumers from algorithmic discrimination in high risk AI systems. While originally slated for February 2026, the enforcement date was recently delayed to June 30, 2026, following a 2025 special legislative session, California's AI Transparency Act and Generative AI Training Data Transparency Act (effective Jan 1, 2026). California's AI Transparency Act mandates that generative AI providers with over $1 million monthly users in the state implement watermarking, content detection tools and clear disclosures for AI-generated content by August 2, 2026. It forces, for the first time, public disclosure of safety protocols, incident reporting, and whistleblower protections for large-scale, frontier AI models, with potential penalties of up to $1 million for violations. The Generative AI Training Data Transparency Act (officially California Assembly Bill 2013 or AB 2013) is a landmark law that requires developers of generative AI systems to publicly disclose summaries of the data used to train their models. Signed into law in September 2024, it became effective on January 1, 2026. Final amendments to the Children's Online Privacy Protection Act (COPPA) took effect in June 2025, enforcing stricter controls on data collection and enhancing parental rights regarding AI usage. New, stringent transparency requirements for Automated Decision-Making (ADM), aimed at eliminating black box decisions, are coming into effect (e.g., Australia's Privacy Act, effective Dec 2026). The DOJ's Bulk Data Rule (2025) and various healthcare related AI laws (e.g., in Texas) are forcing stricter controls on how algorithms are trained and deployed. Deep learning models with opaque decision-making processes make it difficult to audit for bias or explain outcomes, hindering the ability to assign liability when AI causes harm. The hunger of AI models for massive datasets often clashes with data minimization and purpose limitation principles, leading to risks of data misuse, particularly in AI-powered surveillance. Regulators face difficulties proving causation between algorithm design and harm, leading to a shift toward proactive privacy impact assessments rather than just reactive punishment. 2025 marked a shift from testing AI to deploying it, and 2026 is defined by intense, coordinated enforcement, with regulatory, ethical, and legislative frameworks converging globally. Proposed laws in 2026, such as in Alabama, aim to ensure AI cannot be the final arbiter in critical decisions (e.g., insurance claim denials). The no blacker boxes imperative is driving the adoption of tools that make AI systems interpretable to users, particularly in healthcare. A 2026 trend is the requirement that corporate boards take an active, documented role in AI governance and cybersecurity oversight, rather than just receiving briefings.

By 2026, the regulatory environment is characterized by a bumpy road of navigating sometimes conflicting state, federal, and international rules, making comprehensive AI, privacy, and technology compliance a top priority for businesses. Black box algorithms are AI and machine learning systems, particularly deep neural networks, where the internal decision-making process is invisible, opaque, or too complex to understand. Users can observe inputs and outputs but cannot trace how the system reached a specific conclusion. Current laws primarily regulate human behavior, while AI systems possess a degree of autonomy, and their behavior may exceed the direct control of developers and users, complicating issues such as liability determination, intellectual property rights, data protection, and ethics. Furthermore, the lack of transparency in AI system

decision-making may lead to discrimination, and cross border operations may result in legal conflicts. It means that the lack of transparency in AI leading to discrimination and cross border operations causing legal conflicts, are primary ethical and legal challenges in the deployment of AI. Cross border operations involve business, logistics, or authorized activities occurring between two or more countries, such as international trade, manufacturing, or service provision. These activities, which include cross border e-commerce and drone operations, require strict compliance with international, national, and local regulations to manage complex logistics, customs, and documentation. Legal conflicts generally fall into two categories including conflicts of interest (ethical issues for lawyers) and conflicts of laws (jurisdictional disputes). Conflicts of interest arise when a lawyer's duty to a client is compromised by personal interests or other clients. Conflicts of laws occur when a case has connections to multiple jurisdictions, requiring a determination of which rules apply. Multiple jurisdictions refer to legal conflicts, regulatory compliance, or business operations that span across two or more countries, states, or legal systems. This requires coordinating different laws, court systems and regulatory frameworks, particularly in, cross border and cases or multijurisdictional investigations. Multijurisdictional investigations involve coordinated legal, regulatory, or criminal inquiries across multiple countries or states, commonly targeting issues like financial crime, bribery, or data breaches. These complex, high risk cases require specialized legal teams, localized expertise, and careful management of conflicting data privacy laws and, ultimately, regulatory, enforcement, and litigation strategies. Therefore, the development of AI law has become a crucial issue that academia and policymakers urgently need to address (Gibney, 2024; Quintais, 2025; Zou and Zhang, 2025).

2. CORE ISSUES OF AI LAW

(1) Liability Delineation and Legal Personality: AI systems may cause harm during autonomous operation, and current laws struggle to clearly define liability. For example, in the event of a traffic accident involving an autonomous vehicle, liability may involve the vehicle manufacturer, software developer, vehicle owner and traffic management department. Traditional legal systems rely on human behavior as the basis for liability, which cannot fully encompass the autonomous behavior of AI. Autonomous behavior of AI is systems that perceive their environment, set goals, make decisions, and execute actions with minimal or no human intervention. Driven by machine learning and Large Language Models (LLMs) (Cao, et al., 2025), these AI agents operate independently, adapting to new data to improve performance, as seen in self-driving cars, robotics, and complex software agents (Gonzalez et al., 2026). AI agents are autonomous systems powered by the LLMs that perceive their environment, reason through complex tasks, and use tools to achieve specific goals without constant human oversight. Unlike chatbots, which are software applications that simulate human conversation via text or voice, using Natural Language Processing (NLP) to understand user intent, Ranging from basic rule-based systems to advanced Generative AI (LLMs), they automate tasks in customer service, marketing, and, personal assistance, offering 24/7 support and improved operational efficiency, they proactively execute multi-step workflows, such as analyzing data, writing code, or managing processes, representing a shift toward agentic AI. Some scholars have proposed the concept of electronic personality, granting AI limited legal subject status, enabling it to bear responsibility in specific situations. Granting AI is two distinct, emerging

areas: the legal and ethical debate over granting rights or legal personhood to AI systems, and the practical, technical application of using AI in the grant writing and funding process. However, electronic personality remains controversial in practice; issues such as the degree of AI autonomy, predictability, and liability insurance remain unresolved. **(2)** Data Protection and Privacy: AI systems rely on vast amounts of data for training and decision-making, including sensitive personal information such as health data, financial information, and behavioral patterns. Data protection and privacy are core issues in AI law. For example, the EU's General Data Protection Regulation (GDPR) stipulates that the collection, use, and cross border transfer of personal data must adhere to the principles of legality, minimization, and transparency. However, the automated data processing of AI systems may make it difficult to fully implement these principles. **(3)** Intellectual Property (IP) Rights: AI-generated content (such as music, images, code, and scientific articles) raises copyright ownership issues. Traditional intellectual property law, centered on human creators, is difficult to directly apply to AI creations. Different countries have explored different directions: - US Model: Treats AI as a creative tool, with copyright belonging to the human using the AI. - European Model: Some countries are discussing including AI as a co-creator or creative assistant. - Chinese and Japanese Model: Copyright protection for AI-generated works still primarily relies on the human operator. **(4)** Algorithm Transparency and Bias: Lack of transparency in AI decision-making processes can lead to discrimination. For example, AI in recruitment may be biased against women or specific ethnic groups, while AI in lending may be unfair to low-income groups. Legal requirements for AI systems to be transparent, explainable, and traceable are necessary to ensure fairness. **(5)** International Harmonization and Standardization Consistency: AI technology operates across borders, and laws vary significantly from country to country. For example, the EU's GDPR and the US California Consumer Privacy Act (CCPA) differ in their data protection provisions, potentially leading to legal conflicts for multinational corporations. Multinational corporations face complex legal conflicts arising from navigating conflicting national laws, varying ethical standards, tax regulations, and labor compliance across jurisdictions. Main challenges include managing risks related to data privacy, intellectual property, environmental damage, and liability for subsidiary actions, which often require tailored legal strategies. International standardization and cooperation are crucial for AI law. In this article, we focus on the impacts of AI law on economy, technology industry and culture, as well as the relationships between AI law and human behavior, and between fraud and AI law. The previous statements are compiled into **Figure.3**.

3. FUTURE DEVELOPMENT TRENDS AND CHALLENGES OF AI LAW

3.1. Future Development Trends of AI Law

(1) Specialized Legislation and Regulatory Sandboxes: Specialized legislation can design legal norms specifically for the characteristics of AI technology, while regulatory sandboxes allow companies to test AI systems in a controlled environment. AI regulatory sandboxes (Genicot and Moraes, 2025; Qin et al., 2025) are controlled, supervised environments designed for testing innovative AI systems under real-world conditions with regulatory oversight before market deployment. Mandated by the EU AI Act, these frameworks foster innovation, provide legal clarity, and facilitate compliance for small and medium-sized enterprises (SMEs) by allowing temporary deviations from certain regulations, with at least one sandbox required in each EU member

state by August 2, 2026. Some examples include AI regulatory sandboxes in Singapore, the UK and Israel. Singapore is a leader in AI governance, operating specialized regulatory sandboxes to foster responsible innovation. Key initiatives include the Generative AI Evaluation Sandbox (launched Oct 2023) for the LLMs and the Global AI Assurance Sandbox for agentic AI, both aimed at tackling risks like data leakage and bias. The UK is launching an AI Growth Lab with regulatory sandboxes to accelerate AI adoption by testing tools in controlled, real-world environments, with potential for temporary regulatory flexibility. Announced in October 2025, this initiative focuses on sectors like healthcare, transport, and advanced manufacturing to foster innovation and responsible development. Israel is implementing sector-specific AI regulatory sandboxes to foster innovation while ensuring safety, particularly in education and healthcare. These frameworks allow companies to test AI technologies with regulatory guidance, aiming to balance rapid development with ethical, secure, and responsible deployment. This approach balances innovation and public safety, contributing to the gradual improvement of the legal system. **(2)** Legalization of AI Ethics (Radanliev, 2025; Wang and Blok, 2025): AI ethical norms such as restrictions on the use of autonomous weapons, deep fake technology (Wahab, 2025), and surveillance technology (Slobogin and Brayne, 2023), can be gradually incorporated into legal provisions. International organizations and national legislators are promoting relevant legislation to protect the public interest. **(3)** Cross-Sectoral Legal Integration: AI law needs to intersect with intellectual property law, privacy law, labor law, and consumer protection law to form a comprehensive governance framework. For example, AI in medical diagnosis may involve medical regulations, personal data protection law and liability allocation issues, requiring cross sectoral legal collaboration. **(4)** International Standardization and Collaboration: The Organization for Economic Cooperation and Development (OECD) and The United Nations Educational, Scientific and Cultural Organization (UNESCO) promote AI ethics and legal standards, which international companies can use to design compliant AI systems. International collaboration helps to unify regulatory standards and reduce cross border legal risks. The previous statements are compiled into **Figure.4**

3.2. Challenges of AI Law

(1) Rapid Technological Evolution vs. Lagging Laws: The pace of AI technology updates far outpaces the speed of lawmaking, leading to gaps or delays in legislation and impacting regulatory effectiveness. **(2)** Complex Liability Definition: AI's autonomous behavior involves multiple parties, including developers, users, and platform providers, making legal liability allocation difficult. **(3)** Cross-border Legal Conflicts: Different countries have varying legal requirements regarding privacy, regulation, and ethics, requiring companies to comply with multiple laws, increasing compliance costs. **(4)** Over-or Under-Regulation: Over-regulation may stifle innovation, while under-regulation may lead to public safety and ethical risks. **(5)** Social Trust and Public Awareness: Public distrust of AI may hinder legal implementation, necessitating policy transparency and public education. The previous statements are compiled into **Figure.5**

4. DISCUSSION

4.1. The Impact of AI Law on Economy

The AI law on economy is multifaceted, influencing innovation, investment, labor markets, international trade, and market competition. As governments worldwide establish regulatory frameworks for AI, these laws shape not only technological development but also broader macroeconomic and microeconomic outcomes. Several jurisdictions have introduced comprehensive AI regulations, including: AI Act, Executive Order 14110 issued by Joe Biden and the Algorithmic Recommendation Management These frameworks generally focus on risk-based classification, data governance, transparency, accountability, and human oversight. While regulatory approaches differ, all seek to balance innovation with risk mitigation. The positive effects are that clear AI rules reduce regulatory ambiguity, encouraging long-term investment. Firms are more willing to allocate capital when compliance expectations are defined. Regulation can enhance consumer trust in AI systems, increasing adoption in finance, healthcare, and transportation. Trust reduces transaction costs and stimulates demand. Common standards (e.g., safety testing, transparency requirements) reduce fragmentation and enable cross border scalability. Negative effects are that small medium enterprises (SMEs) may struggle with documentation, auditing, and risk-assessment requirements. Overly rigid rules may discourage experimentation, especially in fast evolving AI domains like generative AI. Economically, this tension reflects a trade-off between dynamic efficiency (innovation) and allocative efficiency (risk control) (Kumar et al., 2025). The previous statements are compiled into **Figure.6.**

4.2. The impact of AI law on Technology Industry

The impact of AI law on technology industry has become one of the most significant policy innovation intersections of the 21st century. As governments seek to regulate AI to ensure safety, fairness, and accountability, technology companies must adapt their development strategies, governance models, and market behavior. Major regulatory frameworks such as the EU AI Act, the GDPR, and U.S. initiatives like the Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI illustrate how AI governance is reshaping the global technology landscape (Schmitt, 2022). AI regulation introduces substantial compliance obligations: risk assessments and documentation (especially under the EU AI Act's risk-based classification system), algorithmic transparency and explainability requirements, data governance and bias mitigation standards and cybersecurity and robustness testing. A risk-based classification system (Gasiola, 2025) is a regulatory framework used to categorize products, most commonly medical devices and in vitro diagnostics (IVDs) (Dai et al., 2024), based on the potential health risk they pose to users and the public. Instead of a one-size-fits-all approach, this system ensures that higher risk devices undergo more rigorous, stringent, and costly assessments and monitoring compared to lower risk ones. For large firms such as Microsoft, Google, and Meta, compliance requires expanded legal teams, AI ethics boards, and internal audit mechanisms. Smaller startups may face proportionally heavier burdens, potentially slowing entry into regulated markets. These impacts include increased operational costs, greater emphasis on legal technical collaboration and institutionalization of AI governance frameworks. For innovation Incentives and Constraints, AI law affects innovation in two opposing ways, they are, slow product development cycles, increase uncertainty in research

and experimentation and limit deployment of high risk AI applications. For example, high risk AI categories under the EU AI Act (e.g., biometric identification) require stringent conformity assessments before market entry. For clear legal frameworks can, they are, reduce regulatory uncertainty, increase public trust in AI systems and encourage responsible innovation. Similar to how the GDPR ultimately standardized global data practices, AI law may create harmonized global standards that facilitate cross border AI markets. In the long term, predictable regulation may foster sustainable innovation rather than inhibit it. AI law can reshape industry competition in several ways, for example, large firms with greater resources can more easily comply with complex regulations. This may, entrench dominant players, increase barriers to entry and encourage consolidation. Companies that help shape regulatory standards often gain first-mover advantages. Firms investing early in ethical AI frameworks may influence compliance benchmarks. AI law drives transformation in internal corporate governance, they are, creation of AI ethics committees, mandatory human oversight mechanisms, documentation of training data and model behavior and board-level responsibility for AI risk. The shift moves AI from a purely engineering domain to a legally supervised corporate function. Liability frameworks increasingly hold companies responsible for harms caused by automated decision-making systems. AI systems rely heavily on data regulations such as the GDPR. This needs restrict data collection, retention, strengthen consent requirements and Empower user rights (e.g., right to explanation). This impacts are, AI training dataset availability, cross border data flows, monetization models based on surveillance capitalism and technology companies must shift toward privacy-by-design and federated or synthetic data approaches. AI law elevates ethical AI from a public-relations issue to a legal requirement. Companies investing in, explainable AI (Kauffmann et al., 2025; Nicolson et al., 2025), fairness auditing, transparent model documentation and secure AI infrastructure, may gain consumer trust and institutional contracts. Explainable AI is a set of processes and methods, and it allows human users to understand, trust, and interpret the decisions and outputs created by machine learning algorithms. By providing transparency into black-box models, Explainable AI clarifies the reasoning behind AI actions, ensuring accountability, reducing bias, and enhancing safety in critical applications like healthcare or finance. In this context, regulatory compliance becomes not just a cost, but a strategic asset. AI law also intersects with geopolitics (Pappyshev and Chan, 2026). AI law and regulation are profoundly intertwined with geopolitics, as AI has become a central arena for global power competition, economic sovereignty, and ideological rivalry. The development of AI rules is not merely a technical or ethical endeavor but a strategic move by nations to secure technological leadership, military advantage, and economic influence. For example, democratic regimes emphasize human rights and accountability and authoritarian regimes may prioritize state control and surveillance, as well as export controls and AI safety alliances influence global competition. The regulatory approach adopted by major economies may determine technological leadership patterns in the coming decades. The previous statements are compiled into **Figure.7.**

4.3. The Impact of AI Law on Culture

Laws regulating AI do not merely govern technology and they reshape values, norms, creativity, identity, power structures, and collective imagination (Cajueiro and Celestino, 2026). As regulatory frameworks such as the EU AI Act in the European Union and the Algorithmic Accountability Act in the United States emerge, they

influence how societies define fairness, autonomy, creativity, and responsibility in the digital age. AI law shifts how societies assign responsibility. Traditionally, human actors bear legal and moral accountability. With AI systems making autonomous or semi-autonomous decisions, legal frameworks clarify whether responsibility lies with, developers, deployers, data providers and end users. For example, regulatory approaches like the EU's risk-based model emphasize human oversight and traceability. This reinforces a cultural expectation that technology must remain human-controlled rather than autonomous in moral authority. AI systems influence language, media, beauty standards, hiring, and public discourse. AI laws addressing bias and discrimination aim to protect cultural diversity and minority identities. Algorithms may reinforce dominant cultural narratives. Marginalized groups risk invisibility or stereotyping. Cultural pluralism becomes a legal expectation (Holden, 2024). Fair representation becomes institutionalized. AI law thus becomes a mechanism for safeguarding cultural dignity in algorithmic environments. Generative AI tools challenge traditional concepts of authorship and originality (Li et al., 2025). AI copyright debates affect musicians, writers, and artists globally. The debate surrounding AI and copyright has become one of the most significant legal and ethical confrontations of the digital age, pitting creators, publishers, and artists against major technology companies. At the heart of this conflict is whether AI models can lawfully be trained on copyrighted data and whether AI-generated outputs can be protected by copyright (Quintais, 2025). For instance, copyright disputes involving AI-generated art and music have cultural consequences. AI moderation systems shape online discourse. Legal requirements about content moderation, misinformation, and deep fakes influence speech norms. AI-powered facial recognition and predictive analytics reshape public space culture. Regulations limiting biometric surveillance affect whether societies normalize constant monitoring. For example, debates around facial recognition restrictions in Western democracies contrast with broader surveillance adoption in other regions (Almeida et al., 2022). The previous statements are compiled into **Figure.8.**

4.4. The Relationship between AI Law and Human Behavior

The relationship between AI law and human behavior is dynamic, reciprocal, and co-evolutionary. Legal frameworks governing AI systems influence how individuals, corporations, and governments design, deploy, and interact with intelligent technologies. At the same time, human behavior, shaped by cognitive biases, economic incentives, moral intuitions, cultural norms, political pressures, and technological anxieties, profoundly shapes how AI regulations are conceived, drafted, interpreted, and enforced. Regulatory structures such as the EU AI Act and the GDPR illustrate how legal institutions attempt to anticipate and correct predictable behavioral risks, including automation bias, discrimination, opacity, and over-reliance on algorithmic decision-making (Alon-Barkat and Busuioc, 2023). Conversely, public reactions to rapid advances in generative AI exemplified by systems developed by OpenAI, demonstrate how societal perceptions of risk, trust, and fairness accelerate legislative responses. AI governance therefore cannot be understood purely as a technical regulatory project. it is fundamentally a behavioral and sociotechnical phenomenon in which law and human psychology continuously shape one another (Mesenhöller, 2025; Volosevici and Isbasoiu, 2025). The previous statements are compiled into **Figure.9.**

4.5 The Relationship between Fraud and AI Law

The AI fraud crisis is the rapidly growing use of AI to commit or facilitate fraud at a scale, speed, and sophistication that traditional legal and security systems struggle to control. Advances in machine learning, generative AI, and automated decision systems have created powerful tools that can be misused for deception, identity theft, and financial manipulation. The AI fraud crisis describes a global surge in fraud enabled by AI technologies, including, deepfake impersonation, AI-generated phishing and scams, automated identity theft, financial manipulation and market fraud and synthetic identity creation (Moreno, 2024; Aasimuddin and Mohammed, 2025; Vechietti et al., 2025; Clark and Lewandowsky, 2026). Unlike traditional fraud, AI-enabled fraud can be automated, personalized and massively scalable, allowing criminals to target thousands or millions of victims simultaneously. AI tools can generate, perfectly written scam emails, personalized phishing messages, fake customer service chats and fake legal or banking notices. Traditional phishing often had grammatical errors.

AI-generated scams can appear professional and convincing. Therefore, the relationship between fraud and AI law is becoming increasingly significant as AI systems reshape financial markets (Shpachuk et al., 2026), digital communications, and regulatory enforcement. AI can both facilitate fraud and help detect and prevent it, creating a complex legal and ethical landscape. AI-generated audio, video, and images can impersonate real individuals. For example, deep fake technology has been misused to mimic executives' voices for financial scams. These tools often rely on advanced generative models similar to those developed by companies such as OpenAI although legitimate developers implement strict safeguards. For example, some legal challenges can include proving intent, attributionm and determining liability. AI-driven trading bots can manipulate markets through spoofing, dump-and-dump schemes and automated arbitrage manipulation (Imandojemu, et al., 2025). Regulatory bodies like the U.S. Securities and Exchange Commission increasingly monitor algorithmic trading systems. For Legal issue, when does automated trading cross into criminal fraud? Who is responsible when AI acts autonomously? The LLMs can generate highly personalized scam emails, mimic professional writing styles, and automate large scale deception. This increases the scale and sophistication of online fraud. For core Legal Questions in AI-Related Fraud, who is responsible when AI commits fraud? Most jurisdictions currently treat AI as a tool, not a legal person (Bello and Olufemi, 2024; Hidayati et al., 2025). For ethical and societal implications (Giannopoulos and Li, 2025), They are, AI-driven fraud raises broader concerns, erosion of trust in digital evidence, weaponization of synthetic media and mass automation of deception For future legal developments, Likely trends include mandatory watermarking of AI-generated content, expanded corporate liability standards, stronger cross border enforcement cooperation and AI audit and compliance certification systems. Summarily, AI has transformed fraud from an individual criminal act into a scalable and automated phenomenon. Therefore, AI law must balance innovation, security, accountability and human rights. The previous statements are compiled into **Figure.10.**

4.6. Policy Recommendations

(1). Establish a dedicated AI legal and regulatory sandbox to balance innovation and risk management. Dedicated AI legal refers to the emerging field of legal practice, technologies, and specialized counsel focused on navigating the legal, regulatory, and ethical challenges posed by AI. This field is rapidly maturing, with major law firms creating specialized AI practice groups and hiring AI lawyers to advise on AI-specific compliance, data privacy, and intellectual property (Mansouri et al., 2025). **(2)** Introduce an explainable AI and algorithm auditing system to ensure fair decision-making (Basu and Das, 2025). Fair decision-making involves following transparent, unbiased procedures that allow affected parties to provide input, aiming for equitable outcomes rather than just focusing on results. Key elements include impartiality, handling conflicts of interest, giving notice, providing reasoning, and mitigating bias. It requires a balanced approach to fairness and efficiency, particularly in AI or high-stakes contexts (Decker et al., 2025). **(3)** Strengthen data protection, privacy protection, and cross border collaboration. Strengthening data and privacy protection, along with cross border collaboration, requires implementing robust security measures (encryption, Privacy by Design), adopting frameworks like the Global Cross-Border Privacy Rules (CBPR) system and fostering international, as well as multi-lateral enforcement cooperation. The CBPR System is an international, voluntary, and accountability-based data privacy framework designed to facilitate secure, compliant cross border data flows. Established in 2022 and expanded beyond the Asia-Pacific Economic Cooperation (APEC) region, it allows organizations to certify their privacy practices against high-standard, interoperable data protection requirements. Key actions include regular risk assessments, compliance with laws like GDPR, CCPA, and using tools like the Global Privacy Enforcement Network (GPEN). Fostering international (Tsai, 2011), in a professional context, involves building cross border partnerships, knowledge sharing, and, for example, this LinkedIn article suggests focusing on mutual understanding, transparent communication, and recognizing local strengths to drive innovation and sustainable development. It encompasses international collaboration in research, trade cooperation, and cultural understanding through language exchange. Multilateral enforcement cooperation involves three or more nations, or international bodies, working together to address shared challenges, enforce regulations, and exchange information across borders. This approach is essential for tackling global issues like transnational crime, terrorism, environmental degradation, and financial fraud that no nation can resolve alone (Katzenberg and Kuthiala, 2026). **(4)** Promote the legalization of AI ethical norms, such as restricting autonomous weapons and surveillance technologies. International efforts to restrict lethal autonomous weapon systems (LAWS), often referred to as killer robots, are intensifying, with a growing consensus among many United Nations member states, international organizations, and civil society groups to establish a legally binding instrument by 2026. These weapons are defined as systems that can select and engage targets without human intervention. The core objective of these restrictions is to ensure meaningful human control over the use of force, citing significant legal, ethical, and humanitarian risks. **(5)** Cultivate public trust in AI technology (Afroogh et al., 2024) and enhance education and policy transparency. Policy transparency (Liu et al., 2023) is the practice of making government or organizational policies, data, and decision-making processes open, accessible and understandable to the public. It promotes trust, accountability, and citizen participation by ensuring information is complete, objective, and usable. Key elements include publishing rationale, fostering

dialogue, and allowing scrutiny. Cultivating public trust (Möllering, 2017) is the process of establishing confidence in an organization, government, or institution's integrity, reliability and capability to act in the best interests of the public. It is a proactive, continuous endeavor rather than a one-time project, often described as a shock absorber that allows organizations to adapt and maintain credibility during crises. The previous statements are compiled into **Figure.11**

5. CONCLUSION

The development of AI law is a dynamic and multi-layered process that requires consideration of technological innovation, ethical responsibility, social security, and international coordination. Technological innovation is the development and adoption of new products, processes, or systems that improve efficiency, sustainability, and competitiveness across industries. It acts as a primary driver of economic growth by transforming industries through AI, digitalization, and green technology. It is crucial for businesses to adapt to these changes to avoid becoming obsolete. Ethical responsibility is the obligation to act in accordance with moral principles, such as honesty, fairness, and compassion, to ensure actions positively impact stakeholders and society, rather than causing harm. It involves aligning personal values and professional conduct with societal norms and legal standards. Social Security is a federal program in the United States that provides financial protection through retirement, disability, and survivor benefits. International coordination is the collaboration between nations, financial authorities, and international organizations to align policies, share information, and take joint action to foster global stability, economic growth, and address shared crises. Effective AI law should be forward-looking, flexible, and capable of cross domain coordination to address the various challenges brought about by the rapid evolution of AI. Policymakers need to combine law, technology, and ethics to jointly construct a comprehensive framework for AI governance, promoting a balance between technological innovation and the public interest.

Acknowledgments

In memory of my mother who was dead on 09 October 2016.

Data availability statement: Data sharing is not applicable to this article as no datasets were generated or analysed during the current study

Conflicts of interest: The author declares that there are no conflicts of interest.

Author Contributions: The author contributed to the conceptualization, writing, review and editing of this manuscript.

Funding statement: There is no funding "Not Applicable"

Compliance with ethical statements consisting of conflicts of interest statements and informed consent

(1) All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki Declaration and its later amendments or comparable ethical standards.

(2) The author declares that there are no conflicts of interest.

(3) Informed consent was obtained from all individual participants involved in the study.

(4) This work does not include animals as subjects.

(5) Declaration of generative AI in scientific writing: The author declares no AI in scientific writing.

REFERENCES:

1. Aasimuddin, M. and Mohammed, S., (2025), AI-Generated Deepfakes for Cyber Fraud and Detection, International Journal of Advanced Research in Computer and Communication Engineering, Vol.14 (4), 760- 767, doi: 10.17148/IJARCCE.2025.144108.
2. Afroogh, S., Akbari, A., Malone, E., Kargar, M. and Alambeigi, H., (2024), Trust in AI: progress, challenges, and future directions, Humanities and Social Sciences Communications, Vol.11, 1568, doi: 10.1057/s41599-024-04044-8
3. Ahsen, M. E., Ayvaci. M. U. S., Mookerjee, R. And Stolovitzky, G., (2025), Economics of AI and human task sharing for decision making in screening mammography, Nature Communications, Vol.16, 2289, doi: 10.1038/s41467-025-57409-1.
4. Akila, K., Gopinathan. R., Arunkumar, J. and Malar, B. S. B., (2025), The Role of Artificial Intelligence in Modern Healthcare: Advances, Challenges, and Future Prospects, European Journal of Cardiovascular Medicine, Vol.15 (4), 615 – 624, doi: 10.61336/ejcm/25-04-94.
5. Almeida, D., Shmarko, K. and Lomas, E., (2022), The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks, AI and Ethics, Vol.2, 377–387, doi: 10.1007/s43681-021-00077-w.
6. Alon-Barkat, S. and Busuioc, M., (2023), Human–AI Interactions in Public Sector Decision Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice, Journal of Public Administration Research and Theory, Vol.33 (1), 153–169, doi: 10.1093/jopart/muac007.
7. Basu, D. and Das, U., (2025), The Fair Game: Auditing & debiasing AI algorithms over time, Cambridge Forum on AI: Law and Governance, Vol.1, e27. doi:10.1017/cfl.2025.8.
8. Batty, M., (2025), Generative AI, Environment and Planning B: Urban Analytics and City Science, Vol.52 (5), 1031-1034, doi 10.1177/23998083251332093.
9. Bello, O. A. and Olufemi, K., (2024), Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities, Computer Science & IT Research Journal, Vol.5 (6), 1505-1520, doi: 10.51594/csitrj.v5i6.1252.
10. Boos, A. K., (2024), Conceptualizing Automated Decision-Making in Organizational Contexts, Philosophy & Technology, Vol.37, 92, doi: 10.1007/s13347-024-00773-5
11. Cajueiro, D. O. and Celestino, V. R. R., (2026), A comprehensive review of Artificial Intelligence regulation: Weighing ethical principles and innovation, Journal of Economy and Technology, Vol.4, 77-91, doi: 10.1016/j.ject.2025.07.001.
12. Cao, Z., Zhang, X. and Zeng, D. D., (2025), Large language models: Technology, intelligence, and thought, Frontiers of Engineering Management, Vol.12, 710–715, doi: 10.1007/s42524-025-5004-3.
13. Chen, G., Dang, J. and Liu, L., (2024), After opening the black box: Meta-dehumanization matters in algorithm recommendation aversion, Computers in Human Behavior, Vol.161, 108411, doi: 10.1016/j.chb.2024.108411.
14. Clark, S. and Lewandowsky, S., (2026), The continued influence of AI-generated deepfake videos despite transparency warnings, Communications Psychology, Vol.4, 13, doi: 10.1038/s44271-025-00381-9.

15. Dai, B., Wu, W. and Zhao, B., (2024), The rise of China's in vitro diagnostics industry: Evolution from local innovation to global leadership, VIEW, Vol.5 (6), 20240100, doi: 10.1002/VIW.20240100.
16. Decker, M. C., Wegner, L. and Leicht-Schlten, C., (2025), Procedural fairness in algorithmic decision-making: the role of public engagement, Ethics and Information Technology, Vol.27, 1, doi: 10.1007/s10676-024-09811-4.
17. Gonzalez, G., Habel, J. and Hunter, G. K., (2026), AI agents, agentic AI, and the future of sales, Journal of Business Research, Vol.202, 115799, doi: 10.1016/j.jbusres.2025.115799
18. Gasiola, G. G., (2025), Rebuilding the pyramid: The AI Act's risk-based approach using a binary decision diagram, Computer Law & Security Review, Vol.58, 106189, doi: 10.1016/j.clsr.2025.106189.
19. Genicot, N. and Moraes, T. G., (2025), Exploring the boundaries of AI regulatory sandboxes under the AI Act: Flexibility and real-world testing, Cambridge Forum on AI: Law and Governance, Vol.1, e36, doi:10.1017/cfl.2025.10013
20. Giannopoulos, G. A. and Li, Y., (2025), Ethical and Societal Implications, Human Mobility, Artificial Intelligence and Climate Change, 213–237, doi: 10.1007/978-3-032-08171-1_9.
21. Gibney, E., (2024), What the EU's tough AI law means for research and ChatGPT, Nature, 626 (8001), 938-939, doi: 10.1038/d41586-024-00497-8.
22. Hidayati, M. N., Surono, A. and Pamungkas, E., (2025), Criminal Liability For Ai-Based Cybercrime: Comparative Analysis Of Common Law And Civil Law Approaches, Journal of Law, Politic and Humanities, Vol.6 (2), 1064–1085, doi 10.38035/jlph.v6i2.2683
23. Holden, L., (2024), Cultural expertise and legal pluralism: introduction to the special section, Legal Pluralism and Critical Social Analysis, Vol.56 (2), 167-170, doi: 10.1080/27706869.2024.2384238.
24. Imandojemu, K., Osabohien, R., Al-Faryan, M. A. S. and Odebunmi, S. T., (2025), Artificial intelligence-driven algorithmic trading: Analyzing its impact on stock market volatility in emerging vs. developed economies, Development and Sustainability in Economics and Finance, Vol.8, 100104, doi: 10.1016/j.dsef.2025.100104.
25. Katzenberg, B. and Kuthiala, A., (2026), Innovations in Multilateralism: Reflections on developing INTERPOL's Agreement on Privileges and Immunities, AJIL Unbound, Vol.120, 5-10, doi:10.1017/aju.2025.10043.
26. Kauffmann, J., Dippel, J., Ruff, L., Samek, W., Müller, K. R. and Montavon, G., (2025), Explainable AI reveals Clever Hans effects in unsupervised learning models, Nature Machine Intelligence, Vol.7, 412–422, doi: 10.1038/s42256-025-01000-2.
27. Kumar, A., Shankar, A., Hollebeel, L. D., Behl, A. and Lim, W. M., (2025), Generative artificial intelligence (GenAI) revolution: A deep dive into GenAI adoption, Journal of Business Research, Vol.189, 115160, doi: 10.1016/j.jbusres.2024.115160.
28. Li, W., Song, R., Zhang, B. and Yu, K., (2025), AI creativity and legal protection for AI-generated works in posthuman societal scenarios, Sustainable Futures, Vol.9, 100749, doi: 10.1016/j.sftr.2025.100749.

29. Liu, B., He, S., Lin, S., Zhang, J. and Xue, B., (2023), How usability of policy transparency promotes citizen compliance: evidence from a survey experiment, Journal of Chinese Governance, Vol.8 (4), 473-497, doi: 10.1080/23812346.2023.2166568.
30. Lukács, A. and Váradi, S., (2023), GDPR-compliant AI-based automated decision-making in the world of work, Computer Law & Security Review, Vol.50, 105848, doi: 10.1016/j.clsr.2023.105848
31. Mansouri, O., Yusuf, N. and Kooli, C., (2025), Ethical frontiers and legal boundaries: Proposing a unified framework for AI regulation and accountability, Next Research, Vol.2 (4), 101087, doi: 10.1016/j.nexres.2025.101087
32. Mesenhöller, M., (2025), Exploring the application of Social Practice Theory in technology-related research: A state of the art literature review, Energy Research & Social Science, Vol.126, 104145, doi: 10.1016/j.erss.2025.104145.
33. Miah, M. H., Gupta, S. K., Yali, L., Alsekait, D. M., Alzu'bi, S., Nabil, A., Chowdhury, H. R. and Kanon, M., (2026), AI based decision-making system for tooling design of aircraft product assembly with developed knowledge retrieval algorithm, Scientific Reports, Vol.16, 5393, doi: 10.1038/s41598-025-32936-5.
34. Möllering, G., (2017), Cultivating the field of trust research, Journal of Trust Research, Vol.7 (2), 107-114, doi: 10.1080/21515581.2017.1380912.
35. Moreno, F. R., (2024), Generative AI and deepfakes: a human rights approach to tackling harmful content, International Review of Law, Computers & Technology, Vol.38 (3), 297-326, doi: 10.1080/13600869.2024.2324540.
36. Nicolson, A., Bradburn, E., Gal, Y., Papageorghiou, A. T. and Noble, J. A., (2025), The human factor in explainable artificial intelligence: clinician variability in trust, reliance, and performance, npj Digital Medicine, Vol.8, 658, doi: 10.1038/s41746-025-02023-0.
37. Pappyshev, G. and Chan, K. J. D., (2026), AI regulatory strategies for digital sovereignty: The role of geopolitics and technological disparities, Electronic Markets, Vol.36, 8, doi: 10.1007/s12525-025-00870-z.
38. Qin, Y., Yao, H., Ren, P., Tian, X. and You, M., (2025), Regulatory sandbox expansion: Exploring the leap from fintech to medical artificial intelligence, Intelligent Oncology, Vol.1 (2), 120-127, doi: 10.1016/j.intonc.2025.03.001
39. Quintais, J. P., (2025), Generative AI, copyright and the AI Act, Computer Law & Security Review, Vol.56, 106107, doi: 10.1016/j.clsr.2025.106107.
40. Radanliev, P., (2025), AI Ethics: Integrating Transparency, Fairness, and Privacy in AI Development, Applied Artificial Intelligence, Vol.39 (1), 2463722, doi: 10.1080/08839514.2025.2463722.
41. Schmitt, L., (2022), Mapping global AI governance: a nascent regime in a fragmented landscape, AI and Ethics, Vol.2, 303–314, doi: 10.1007/s43681-021-00083-y.
42. Shpachuk, V., Markova, O. and Adamyk, B., (2026), AI-driven financial fraud: key risks and legal protections for financial institutions, Journal of Banking Regulation, Vol.27, 6, doi: 10.1057/s41261-025-00304-y.

43. Slobogin, C and Brayne, S., (2023), Surveillance Technologies and Constitutional Law, Annual Review of Criminology, Vol.6, 219-240 doi: 10.1146/annurev-criminol-030421-035102.
44. Triguero, I., Malina, D., Payatos, J., Ser, J. D. and Herrera, F., (2024), General Purpose Artificial Intelligence Systems (GPAIS): Properties, definition, taxonomy, societal implications and responsible governance, Information Fusion, Vol.103, 102135, doi: 10.1016/j.inffus.2023.102135.
45. Tsai, S. P., (2011), Fostering international brand loyalty through committed and attached relationships, International Business Review, Vol.20 (5), 521-534, doi: 10.1016/j.ibusrev.2010.10.001
46. Van Quaquebeke, N., Tonidandel, S. and Banks, G. C., (2025), Beyond efficiency: How artificial intelligence (AI) will reshape scientific inquiry and the publication process, The Leadership Quarterly, Vol.36 (4), 101895, doi: 10.1016/j.leaqua.2025.101895.
47. Vechietti, G., Liyanaarachchi, G. and Viglia, G., (2025), Managing deepfakes with artificial intelligence: Introducing the business privacy calculus, Journal of Business Research, Vol.186, 115010, doi: 10.1016/j.jbusres.2024.115010
48. Vivo, P., Katz, D. M. and Ruhl, J. B., (2025), CompLex: Legal systems through the lens of complexity science, Europhysics Letters, Vol.149 (2), 22001, doi: 10.1209/0295-5075/ad99fc.
49. Volosevici, D. and Isbasoiu, G. D., (2025), Surveillance as a Socio-Technical System: Behavioral Impacts and Self-Regulation in Monitored Environments, Systems, Vol.13 (7), 614, doi: 10.3390/systems13070614.
50. Wahab, A., (2025), Futures of Deepfake and society: Myths, metaphors, and future implications for a trustworthy digital future, Futures, Vol.173, 103672, doi: 10.1016/j.futures.2025.103672
51. Wang, H. and Blok, V., (2025), Why putting artificial intelligence ethics into practice is not enough: Towards a multi-level framework, Big Data & Society, Vol.12 (2), 1–14, doi: 10.1177/20539517251340620.
52. Yang, Y., Negash, N. M. and Yang, J., (2025), Recent Advances in Interactive Driving of Autonomous Vehicles: Comprehensive Review of Approaches, Automotive Innovation, Vol.8, 304–334, doi: 10.1007/s42154-024-00332-w.
53. Zou, M. and Zhang, L., (2025), Navigating China's regulatory approach to generative artificial intelligence and large language models, Cambridge Forum on AI: Law and Governance, Vol.1, e8, doi: 10.1017/cfl.2024.4

Figure Captions

Figure 1: Artificial Intelligence (AI)

Figure 2: Generative AI

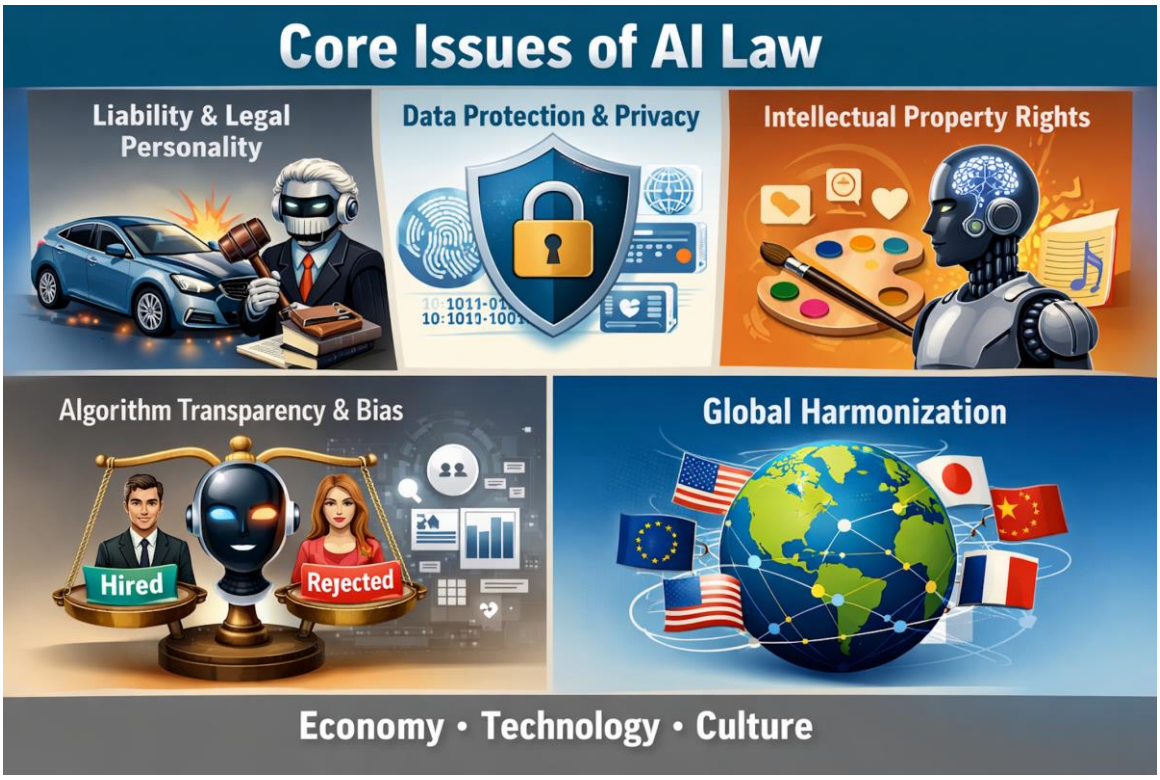

Figure.3: Core issues of AI law.

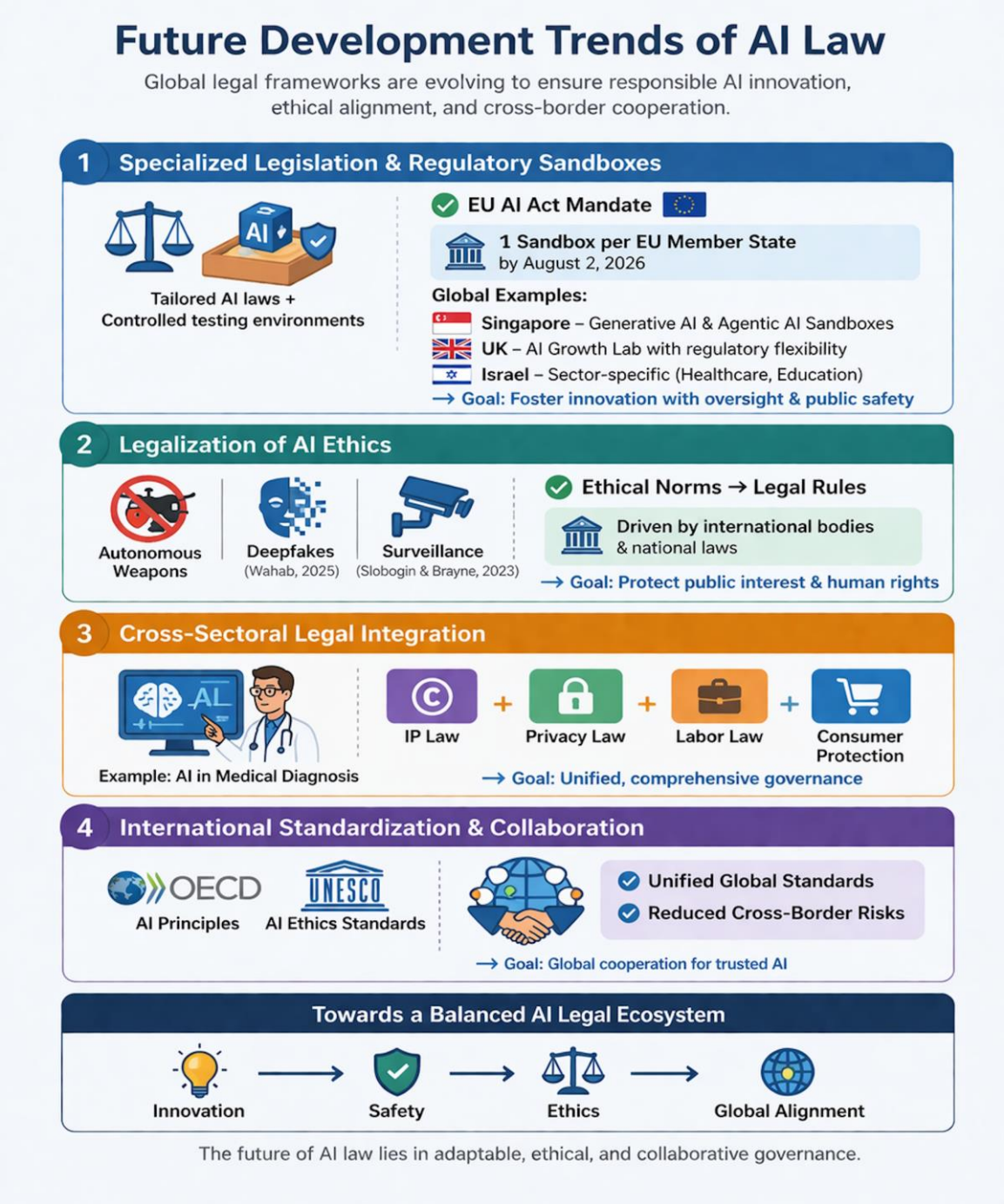

Figure.4: Future development trends of AI law.

Figure.5: Challenges of AI law.

Figure.6: The impact of AI law on economy

Figure.7: The impact of AI law on technology industry

Figure.8: The impact of AI law on culture

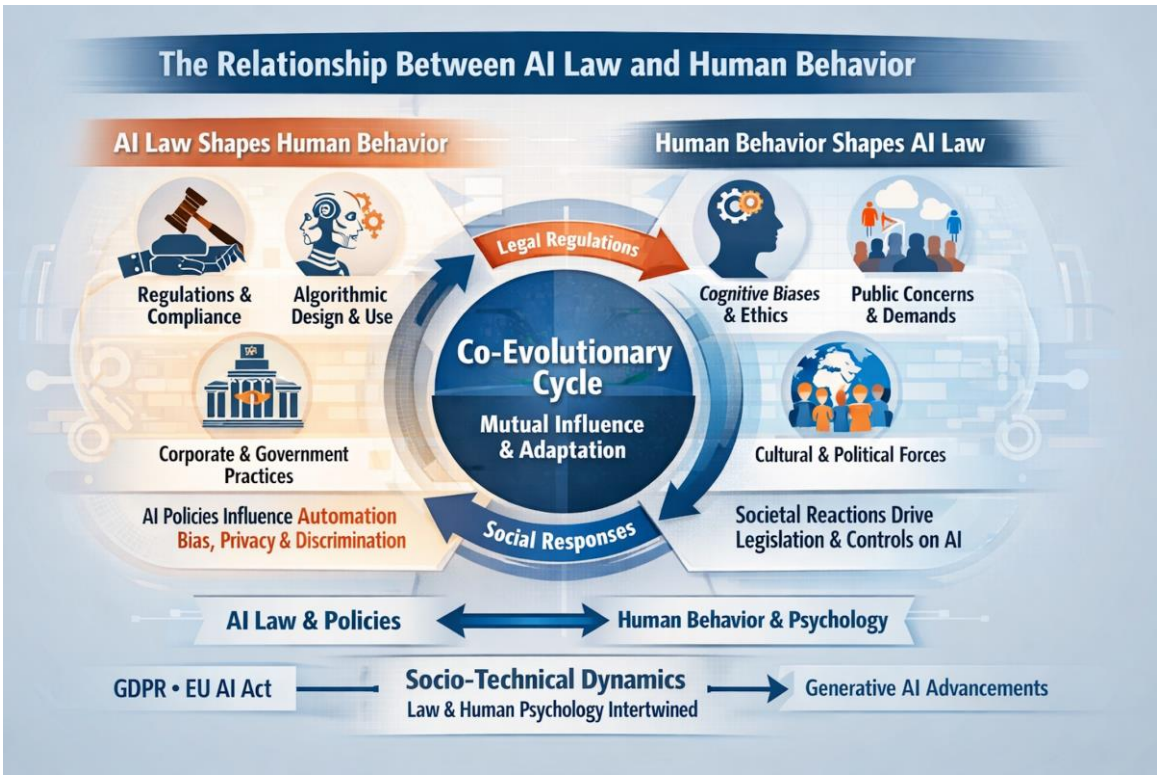

Figure.9: The relationship between AI law and human Behavior

Figure.10: The relationship between fraud and AI law

Figure.11: Policy recommendations