Department of Economics and Finance

Chair of Law and Economics (Business and Corporate Law; Antitrust and Regulation)

AI and Corporate Governance:

Challenges and Potential

Supervisor	Candidate
Prof. Avv. Pierluigi Matera	Arianna Tosti - 278021

Academic year 2024/2025

Table of contents

1. Introduction

Artificial intelligence is transforming the current world, by enhancing discoveries and improvements in mostly all industries. Because of the various renewed AI applications, it has arisen the need for legal frameworks to adapt to the change and, to build reliable legal standards and regulations to take into consideration when evaluating a challenge posed by AI.

Different countries have applied different frameworks. European Union for instance, has adopted a comprehensive regulation based on a risk-approach. United States instead, have decided to rely on their usual fragmented framework, by applying general standards and encouraging States and companies to self-regulate. China and Russia alternatively, even though being far behind EU's and US' legislations, due to political and societal matters, are trying to catch up. However, in general, a lot of issues about AI regulation are still open. The imposition of liability for AI systems' errors is an example, together with the of application of copyright (to what extent the emulation of content is declared to be "fair use").

This paper has the aim to go deeper over these matters and to analyze them.

In particular, it is divided in 7 sections: in the second section, the main types of Artificial Intelligence are described, with a focus on the applications in the legal sector. Nowadays AI is indeed used to perform a lot of tasks, such as legal research, contract automation and the evaluation of M&A's feasibility. And, all of this is allowed thanks to the ability of AI to execute analysis such as due diligences and risk assessments.

In the third section, there is the description of the regulations on AI in the main countries moving for the purpose. So, an analysis towards the European Union, United states, China and Russia and their differences and similarities is done. This section also addresses the theme of a possible global legal framework and, highlights the one that has been reached among some countries.

Moreover, section 4 is about the imposition of liability, a hugely hot topic nowadays. It explores one of the main standards in US Corporate law, the *Caremark* Standard for corporate oversight. It is analyzed by making in a comparison with the regulations on liability in other countries. In this part they are also presented the new and most revolutionary forms of companies, the Decentralized Autonomous Organizations (DAOs), characterized by a great amount of regulation uncertainty.

In section five then, it is presented a line of cases about the most important lawsuits on AI nowadays. A lot of these cases are ongoing, indeed this section, as will be further examined in section 6, has the aim to provide examples of the current gaps in AI law, which are indeed challenging the judgement of the courts.

Section six tries to navigate future possible applications of AI in law firms and their feasibility. Also gaps in the current laws are examined, with an interesting critic to the AI Act provided by the Yale Journal of Law and Technology.

In the end, section seven provides the conclusions extracted from the work.

AI technologies and algorithms are still far ahead of current legislation. Their uses and applications have strongly been enhanced as of today, though, it may not be so recommendable in some cases. Regulation frameworks are trying their best to adapt to this new condition of fast development of AI tools. Some of them are entertaining a safer approach, such as Europe, even though risking to be too strict in the matters. While others may adopt a more open and innovative perspective, like US, but which could potentially be considered too deregulatory. The truth lies somewhere in the middle, and the only possible thing to do right now, is to remain tuned.

2. AI Deployment across industries

The contemporary business environment is becoming highly globalized, with larger workforces that face constantly increasing challenges, ranging from operational inefficiencies to complex decision-making processes. For this reason, for businesses it is of utmost importance to be able to adapt to the new technologies, market demands, and competitive pressures. And in these terms, Artificial Intelligence (AI) has evolved sharply, becoming an indispensable tool for organizations[1].

Businesses often face difficulties in terms of data overload, inconsistent decision-making, resource allocation inefficiencies and, need for real-time insights. Because of these problems indeed, the overall success of an enterprise could really be compromised and, its efficiency may be highly affected. In the current era of digital acceleration, AI may serve as a strategic ally to mitigate such challenges and, its uses can really vary across multiple industries[2].

The transformative impact of AI is reshaping traditional workflow paradigms, from healthcare and finance to manufacturing and retail. Machine Learning (ML) algorithms indeed, through their advanced automation, have the real potential to allow businesses to streamline their operations, to optimize their resource utilization and, to gain insights about consumer behavior and market trends[3]. The latest McKinsey Global Survey on AI[4], finds that organizations are beginning to take steps towards the integration of AI and ML algorithms into business processes. The renewed workflows indeed, tend to include Generative AI (GenAI) in operations and, locate senior leaders in critical roles such as overseeing AI governance. The findings also show that organizations are working to deal with the growing GenAI related risks and, are both hiring new AI-related roles and training preexisting employees to participate in AI deployment. The majority of respondents declare that AI is used in at least one business function in their organizations. As expected, companies with a minimum of $500 million in annual revenue are changing more quickly than smaller organizations, but it is already a result that bodes well. Another element that emerged from the survey, is that the most common type of Artificial Intelligence applied and used in companies is Generative AI, capable of generating content, starting from inputs and information provided[5].

[1] *See* Akash Takyar & LeewayHertz, *AI Use Cases & Applications Across Major industries*, A HACKETT GROUP COMPANY, https://www.leewayhertz.com/ai-use-cases-and-applications/ .
[2] *Id.*
[3] *Id.*
[4] *See* Alex Singla et al., *The State of AI: How organizations are rewiring to capture value* (2025), QUANTUMBLACK AI BY MCKINGSEY, https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai#/ .
[5] *Id.*

Moreover, a research conducted by Adib Bin Rashid and MD Ashfakul Karim Kausik, about "AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications"[6], suggests that the global AI software market is projected to reach $126 billion by 2025, by increasing the enterprise adoption by 270 compared to the last four years. So, the market is expected to extend to a size of $22.6 billion, by powering 95 % of customer interactions by 2025[7].

In their article, Rashid and Kausik believe that this era of businesses and industries focusing on automation and machinery for manufacturing and workforce optimization, can be regarded as the "Fourth Industrial Revolution"[8]. They argue that this transformation in the AI field, is "turning the whole world upside down"[9], by replacing humans and establishing new and more efficient ways of managing industrial and business processes. After all, AI technologies have always tried to improve human needs such as safety and security and, this, coupled with the human-centric focus, has improved resilience and increased emphasis on sustainability[10].

AI has established itself as a transformative force able to boost productivity, save costs, and increase efficiency. Its continuous learning capabilities ensure its adaptability to evolving business landscapes and, thus its application in a large range of sectors in today's world. Starting for instance from healthcare applications, such as patient care, automated diagnosis, and drug discovery, it may also play a pivotal role in finance, in terms of detecting fraud, automating trading, identifying abnormalities in financial transactions, performing risk assessments and optimizing portfolios[11].

Even retail and manufacturing can be boosted. The former indeed, is assisted by personalized shopping experiences, identification of customer preferences, customer support and inventory management. While, the latter can benefit from the analysis and prediction of equipment maintenance

[6] *See* Adib Bin Rashid et al., *AI revolutionizing industries worldwide: a comprehensive overview of its diverse application*, 7 Hybrid Advances 2 (2024).

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *See supra note 1.*

needs, control of quality and optimized supply chains[12]. Not to mention the legal sector, in which AI is revolutionizing sectors such as legal research, contract automation, M&As and dispute resolution[13]. The last two sectors which are worth presenting are energy and, transportation and logistics. In the first one, AI agents may be developed to optimize energy consumption in buildings, factories and transportation. While, in the second many doors are opening, starting from autonomous vehicles and route optimization and going on with AI copilots, reduced fuel consumption and optimized transportation logistics[14].

An early example of a company that uses AI to enhance efficiency and save costs is JPMorgan Chase. It has now been using Artificial Intelligence and Machine Learning for quite some time, to detect fraud and create other kinds of data driven values for customers. Given its early success and the rapid AI-driven advances of large tech companies, the firm made the strategic decision to accelerate AI adoption by building its own platform, OmniAI. It has been developed by the firm's Chief Technology Office, and it is now receiving industry recognition. In 2020, the platform won the CIO 100 Technology Award and was named "Most Cutting-Edge IT Initiative" at Waters Technology's American Financial Technology Awards (AFTAs)[15].

OmniAI is used to solve problems for the firm's data scientists. It finds the data needed, provides access to the compute environments to test and train their models and, avoides duplication of effort in different parts of the enterprise. It allows firms to use AI at a scale, by standardizing processes and providing the security controls. The platform reduces the time it takes the firm to extract and analyze insights about the customers, by allowing it to reduce lots of operational costs and to better serve clients. OmniAI represents a major step forward in the current technology journey [16].

[12] *See supra note 1.*
[13] *See* Lexin Legal Law, *The Legal Future: Artificial Intelligence And Corporate Law (2025),* MONDAQ, https://www.mondaq.com/turkey/corporate-governance/1566104/the-legal-future-artificial-intelligence-and-corporate-law.
[14] *See supra note 1.*
[15] *See* J.P Morgan Chase, *Omni Means "All"*, J.P. MORGAN CHASE, https://www.jpmorgan.com/technology/news/omni-ai.
[16] *Id.*

2.1 AI in Corporate and Business Law

Nowadays, the rapid evolution of technology and specifically Artificial Intelligence, has transformed many industries across the globe and, one of the sectors that have undergone major changes is the legal one. With companies increasingly integrating AI in their business operations, particularly in decision-making and management, traditional legal frameworks face unprecedented opportunities and challenges[17].

In the corporate context, for a great number of tasks, AI tools have really begun to play a pivotal role. There may be pointed out for instance the analysis of large datasets for informed decision-making, the draft of contracts to ensure compliance with existing regulatory frameworks, the prediction of market trends to guide strategic planning and, the support of boardroom and corporate decisions[18].

However, integrating AI into corporate governance, raises fundamental legal doubts. It is indeed still questioned the extent of its legal authority, so whether AI should be granted legal personhood. The imposition of liability in decision-making also represents a problem, together with the importance of oversight of AI systems and their ability to comply with corporate regulations. Governments in the future may need to establish regulatory frameworks for autonomous AI systems, ensuring transparency and accountability in decision-making processes[19].

One of the most debated issues is whether AI systems can replace human directors on corporate boards. There are some cases in which it has already been implemented. An example is the system "Vital", an AI algorithm of an Hong Kong-based venture capital firm[20]: Deep Knowledge Ventures, (a company specialized in biotechnology and medicine), to which it was given the observer status on the board[21].

[17] *See supra note 13.*

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *See* Rossana Miranda, *Ecco Vital, il primo robot consigliere di amministrazione*, 2014 Formiche 1.

But still, even though AI offers unparalleled data analysis capabilities, it lacks the emotional intelligence, ethical reasoning and legal accountability required to human directors. For this reason, in most jurisdictions corporate directors must be natural persons[22].

However, the potential of AI in corporate governance is huge. It may improve decision making by being able to process huge amounts of data in real time, it may predict market trends to guide investment strategies, or it may even identify risks in M&As. This way, operations such as contract analysis and regulatory compliance are streamlined and, time-consuming tasks and costs are reduced[23].

Moreover, another recent development in the corporate world is the emergence of Decentralized Autonomous Organizations (DAOs). They are entities which use blockchain technology to operate without centralized control, relying on smart contracts for governance. Due to their decentralized nature, they face unique legal challenges[24].

The main uses of Artificial Intelligence in the corporate sector are: legal research and E-Discovery, contract automation, M&A and due diligence and, litigation prediction[25].

2.1.1 Contract automation

"Contract management is the discipline used to help legal professionals to create and oversee a contract throughout its lifecycle"[26].

Nowadays, they are available AI tools able to support legal professionals in their work, which allow them to streamline and automate processes, reduce costs and in some cases, enhance accuracy and efficiency[27].

[22] *See supra note 13.*
[23] *Id.*
[24] *Id.*
[25] *See* Philipp Rosenauer et al., *Artificial Intelligence Revolutionising corporate legal departments*, PWC, https://www.pwc.ch/en/insights/regulation/ai-revolutionising-corporate-legal-departments.html.
[26] *See* Bloomberg Law, *Can AI Write Legal Contracts?* (2024), BLOOMBERG LAW, https://pro.bloomberglaw.com/insights/technology/can-ai-write-legal-contracts/#contract-automation-tools .
[27] *Id.*

For instance, legal teams can encounter version control issues when a lot of members are working on the same contract. Tracking obligations and deadlines during the contract review and negotiations can be very difficult and rime-consuming. So, here come into play contract management software (CMS) solutions, designed to automate and streamline the contract management process. They offer a platform for legal and business teams to draft, negotiate, sign, and report business contracts[28]. Moreover, AI technologies such as Natural Language Processing (NLP) and Machine Learning (ML) are fundamentally revolutionizing legal works, by enabling computers to comprehend human language and analyze text sentiment[29].

To automate contract analysis, it is important to train at the best these tools, in order to follow the specific workflows and contract formats that the firm uses. AI-powered technology may reliably draft contracts by using the existing legal documents as a frame of reference. Furthermore, depending on the tool, specific areas of the contracts can be highlighted or not and, at the end, the firm may edit the result to meet the its standards for accuracy and compliance[30].

Nowadays, according to the platform *Cimphony*, there are 10 main automation and AI tools for contract drafting. They are: LowTech AI, Paxton AI, Taskade AI Legal Document Drafting, AGRE+, Definely, DocDraft AI, Amto AI, MyCase IQ, Genie AI and Spellbook [31].

However, a fundamental point that must always be remembered is that AI tools, at least until now, do need the revision and oversight of humans, because they are not sufficiently developed to review a contract alone in its entirety yet. And in these terms, Patrick Lavan, the Bloomberg Law marketing manager, states that: "Right now, there isn't AI technology that's good enough to blindly write a contract without an attorney reviewing it at all. It would be a massive risk for a lawyer to do this because the technology just isn't there yet"[32]. He believes that even though Large Language Models

[28] *See supra note 26.*

[29] *See* Virtasant, *AI Contract Management: 80% Time Savings in Legal Work* (2025), ENTERPRISE AI TODAY, https://www.virtasant.com/ai-today/ai-contract-mangement-legal .

[30] *See* Erin Walker, *AI Contract Drafting & Automation Tools for Lawyers* (2025), CLIO BLOG, https://www.clio.com/blog/ai-contract-drafting-and-automation/.

[31] *See* Cimphony, *Top 10 AI Legal Drafting Tools 2025: Features & Pricing* (2025), CIMPHONY, https://www.cimphony.ai/insights/top-10-ai-legal-drafting-tools-2024-features-and-pricing .

[32] *See supra note 26.*

(LLMs) work well, they are not able to perceive the context as a human attorney would. These tools only act basing on the information provided, so they can be a starting point he believes, but the work has always to be completed by a real lawyer[33].

The use cases for AI rise ethical concerns about the way in which Machine Learning models obtain data (From public domain sources or private ones). So, in any case, transparency about when and how AI tools are used is fundamental[34].

2.1.2 M&A and Due diligence

"Mergers and acquisitions (M&As) are transactions in which the ownership of companies or of their operating units, including all associated assets and liabilities, is transferred to another entity"[35].

In the context of M&As, there are a lot of tasks that may be carried out by AI, which enable to streamline processes and avoid time-wasting[36].

First of all, deal sourcing may be enhanced. Indeed, AI-powered algorithms can analyze vast amounts of data to identify potential targets or buyers that align with specific criteria. Moreover, AI makes it possible to perform smarter due diligence. Financial documents and contracts can be quickly reviewed, informed decision making is enhanced and risks and opportunities can be identified[37].

Another important opportunity is provided by AI's ability to predict analytics. It can analyze historical M&A's data to recognize patterns and predict future deal outcomes, by helping stakeholders to forecast potential challenges and optimize deal structures. Also post-Merger Integration is enhanced. By automating repetitive tasks, identifying synergies to create value and consolidating systems and processes, AI can really ease post-merger integration[38].

[33] *See supra note 26.*

[34] *See supra note 30.*

[35] *See* Gartner, *Mergers and Acquisitions (M&A)*, GARTNER, https://www.gartner.com/en/finance/glossary/mergers-and-acquisitions-m-a- .

[36] *See* Redcliffe Training, *AI in M&A: How It's Changing Mergers & Acquisitions* (2024), REDCLIFFE, https://redcliffetraining.com/blog/ai-in-manda.

[37] *Id.*

[38] *Id.*

A good example of boosting productivity with AI is given by the company Centerline, which, by leveraging Generative AI tools such as V7 for data extracting and automated document analysis, has increased its productivity by 35% in one month in 2024[39].

Among the best and most used AI-powered tools used in M&A automation, according to the platform *Legalfly,* there are: Data site Diligence, an AI virtual data room for M&A, Alpha Sense, an AI-powered market intelligence and document search and Grata, an AI-powered private company search engine[40].

However, while AI has a tremendous potential to revolutionize the M&A landscape, the team of the corporate finance and banking training provider Redcliffe Training believes that it is essential to acknowledge its limitations and challenges. First of all, the quality and availability of the insights on which AI algorithms rely on, is not always guaranteed. Incomplete or inaccurate data can lead to erroneous analyses and potentially misguided decision-making. Moreover, the decision-making process in M&As often involves complex human variables that are difficult to quantify. AI algorithms can not easily capture human factors like culture fit, strategic alignment or personal relationships, thus requiring human supervision[41].

Ethical concerns are also rising. Data privacy, security and transparency are being questioned with the use of AI. And, risks related to unintended biases or discrimination in decision-making, are growing. M&A practitioners are exposed to legal and reputational risks because of the training of AI algorithms based on biased patterns that were present in the past[42].

In the end, in order to address such problems, robust governance frameworks and, adherence to ethical guidelines are required. As AI continues to evolve and become more sophisticated, its impact on the M&A landscape is only set to grow. Through the embracement of AI for M&As, professionals can reach higher efficiency, unlock relevant opportunities and achieve better outcomes for all stakeholders involved[43].

[39] *See* Casimir Rajnerowicz, *AI in Due Diligence: What It Means for M&A and Beyond* (2024), V7 LABS, https://www.v7labs.com/blog/ai-due-diligence.

[40] *See* Gabby MacSweeney, *The top 7 AI tools for M&A due diligence* (2025), LEGALFLY, https://www.legalfly.com/post/the-top-7-ai-tools-for-m-a-due-diligence.

[41] *See supra note 36.*

[42] *Id.*

[43] *Id.*

2.1.3 Legal research and E-discovery

"E-Discovery, short for electronic discovery, refers to the process of identifying, collecting, and producing electronically stored information (ESI) during legal proceedings"[44].

AI can provide for a valuable contribute in this field. Indeed, thanks to all the tools available, among which chatbots and virtual assistants hold a relevant position, vast datasets may be quickly processed and important insights may be found. According to the platform *Legalfly*, among the most popular systems for legal research, there are Bloomberg Law, Lex Machina, Westlaw and Harvey AI[45].

Nowadays, attorneys tend to rely on a variety of research, including court opinions that may support their arguments, materials from similar federal or state cases, state-level legal standards and the background and history of the presiding judge or opposing counsel[46].

However, AI research tools, may have some limitations and risks, mostly in matters of data privacy concerns, misinterpretation of legal judgements, and consequent inaccuracy of results[47].

As the article published in Bloomberg Law: "Can AI do legal research?"[48] has indeed pointed out, AI cannot replace human expertise and judgement and, major ethical concerns for legal professionals could arise. For instance, there may be cases in which AI tools experience "Hallucinations", so phenomena by which AI chatbots confidently provide false information in response to a prompt[49]. Or, in some occasions, it has been demonstrated that the use of AI for legal purposes has strongly been misleading and dangerous. It may be cited a relevant example in which a New York team of lawyers have cited inexistent court cases in their attempt to prove their point to the court. The case in

[44] *See* Bob Dillen, *How AI transforms document review in eDiscovery*, KPMG, https://kpmg.com/ch/en/insights/cybersecurity-risk/e-discovery.html .

[45] *See* Gabriel MacSweeney, *The best AI tools for legal research in 2025* (2025), LEGALFLY, https://www.legalfly.com/post/best-ai-tools-for-legal-research-in-2025#:~:text=AI%20can%20deliver%20tailored%20analyses,need%20when%20you%20need%20it .

[46] *See* Bloomberg Law, *Can AI do legal research?* (2024), BLOOMBERG LAW, https://pro.bloomberglaw.com/insights/technology/can-you-use-ai-for-legal-research/ .

[47] *See supra note 45.*

[48] *See supra note 46.*

[49] *Id.*

question is *Mata v. Avianca, Inc.*[50] of 2023. It was discovered that the attorneys had asked ChatGPT a support for their research without actually verifying it and thus, getting a fine from the judge[51]. Ultimately, a study conducted by Stanford University[52], alarms that there is not enough rigorous and transparent benchmarking of legal tools to make them trustworthy. Few details are published by companies about their AI systems and there are not sufficient standards to evaluate them. A landmark case that the study cites is when the large law firm Paul Weiss spent nearly a year and a half testing a product, but did not develop metrics to evaluate it. For this purpose, a guidance on executives' duty of supervision over products created by AI was recently released by the Bar Associations of California, New York and Florida. So that as of May 2024, more than 25 federal judges have issued standing orders instructing attorneys to disclose or monitor the use of AI in their courtrooms[53].

2.1.4 AI litigation prediction

"Predictive analytics involves using AI and machine learning algorithms to analyze large datasets, including past case rulings, legal findings, judicial decisions and even jury behavior"[54]. It serves to predict future legal outcomes and guide strategies by identifying patterns and trends. For instance, it can help evaluate the risks associated to trial versus settling, or it can highlight potential weaknesses in a case and provide insights on likely timelines and costs[55].

According to the BBC, in 2016, a study conducted at the London College of Law and at the universities Sheffield and Pennsylvania showed that AI was able to predict the outcome of 584 cases

[50] Mata v. Avianca, Inc., 1:2022cv01461 U.S 1 (2023).
[51] *See* Benjamin Weiser, *Here's What Happens When Your Lawyer Uses ChatGPT,* 2023 NY Times 1.
[52] *See* Faiz Surani et al., *AI on Trial: Legal Models Hallucinate in 1 out of 6 (or More) Benchmarking Queries* (2024), STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, https://hai.stanford.edu/news/ai-trial-legal-models-hallucinate-1-out-6-or-more-benchmarking-queries .
[53] *Id.*
[54] *See* Ashley Hallene et al., *Using AI for Predictive Analytics in Litigation* (2024), AMERICAN BAR ASSOCIATION, https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2024-october/using-ai-for-predictive-analytics-in-litigation/ .
[55] *Id.*

with 79% accuracy[56]. This technology indeed enhances lawyers' work by facilitating decision-making processes, by assessing risks and by providing accurate advices to clients. Corporate Law can benefit a lot from AI predictions. Those can estimate the success rate of M&As, the likelihood of shareholder litigation and the probability of regulatory approval for new business ventures[57].

Despite its benefits though, AI-driven legal predictions come with challenges. Their accuracy for instance, depends heavily on the quality of data used to train AI. Not to mention the constant need for human oversight that such a platform would need. So, even though the results in this particular field have been quite promising, with systems such as Pre/Dicta demonstrating the 85% of accuracy rate of their predictions[58], it is always important to let the client understand that such numbers are always an average, and the precise result is not guaranteed[59].

There are three tiers of expertise and accuracy of AI prediction tools. The top tier is highly specialized and highly data-rich, thus performing high-level legal analytics. It includes tools such as Epiq and Lex Machina. The mid-tier is less data-rich but provides more in-depth information. And lastly, the third tier comprises more general AI platforms such as ChatGPT, Gemini, Claude, or LLaMA[60].

Even AI mediation in some fields is on the rise, with chatbots increasingly assisting human mediators in resolving disputes. However, the potential for AI systems' hallucinations, is still too high[61].

3. AI Regulation

[56] *See* Jane Wakefield, *AI predicts outcome of human rights cases (2016),* BBC, *https://www.bbc.com/news/technology-37727387* .

[57] *See* Amy Swaner, *Using AI to Predict Legal Outcomes: A Powerful New Tool for Lawyers* (2024), AI FOR LAWYERS, https://aiforlawyers.substack.com/p/using-ai-to-predict-legal-outcomes .

[58] *Id.*

[59] *See* Dan, *AI-Powered Legal Case Outcome Prediction: Transforming Legal Practice* (2025), PRE-DICTA, https://www.pre-dicta.com/ai-powered-legal-case-outcome-prediction-transforming-legal-practice/#:~:text=These%20predictive%20analytics%20enable%20attorneys,streamline%20litigation%2C%20and%20enhance%20advocacy.

[60] *See supra note 57.*

[61] *See* Katie Shonk, *AI Mediation: Using AI to Help Mediate Disputes* (2025), DAILY BLOG, PROGRAM ON NEGOTIATION - HARWARD LAW SCHOOL , https://www.pon.harvard.edu/daily/mediation/ai-mediation-using-ai-to-help-mediate-disputes/ .

AI is transforming a vast range of industries, including finance, healthcare, law and manufacturing. It is potentially a powerful driver of economic growth and a key enabler of public services[62].

Through the application of AI core principles and rules, company leaders can gain an incredible advantage in the marketplace. Those actions indeed allow a company to instill confidence in customers and regulators. It can also help companies anticipate the governance needs and compliance requirements that may apply to their development and use of AI, by making them more agile[63].

However, it may be difficult to govern this rapidly evolving technology, since the existing legal frameworks and judicial precedents have been designed for a world where the application of AI has negligible impact on society and on businesses[64].

The accelerating capabilities of Generative Artificial Intelligence (GenAI), including Large Language Models (LLMs) and the various AI systems in general, have pushed AI regulation to be one of the main issues for policy makers and regulators nowadays. The risks and unintended consequences of Artificial Intelligence are real and should be taken care of[65].

The main matters to analyze are AI platforms' risks to reinforce human biases, to compromise data security, to produce disinformation or to destabilize financial systems. For instance, a text-generation engine able to imitate other sources is open to misuse. The same applies for voice-imitation softwares, which can mimic an individual's speech patterns to convince a bank or a workplace and, for chatbots, which may be used to cheat in tests, or to give erroneous information. In short, the potential of AI may be disruptive if no limits are posed. So, legislators and regulators are starting to develop frameworks to maximize AI benefits in society, while mitigating risks[66].

Even though the various countries all over the world have adopted different regulations, there are some patterns that are common among all of them. The consistency with the OECD (Organization

[62] *See* EY Global, *How to navigate global trends in Artificial Intelligence regulation* (2024), EY GLOBAL, https://www.ey.com/en_gl/insights/ai/how-to-navigate-global-trends-in-artificial-intelligence-regulation.

[63] *See supra note 62.*

[64] *See* Anand Kumar et al., *AI and Business Law: Navigating New Frontiers*, 67 Calif. Manag. Rev. 1 (2024).

[65] *See supra note 62.*

[66] *Id.*

for Economic Co-operation and Development)'s principles for AI for instance, which have been endorsed by the G20 and, which include the respect for human rights, sustainability, transparency and strong risk management. Moreover, regulations are adapting to the perceived risks around AI and its core values of privacy, non-discrimination, transparency and security. Thus, the level of risk should be proportionate to the directives. Depending on the various AI use cases, there is also the distinction between countries which focus more on sector-specific rules and those with a sector-agnostic regulation. Indeed, they are present some digital policy priorities, such as cybersecurity, data privacy and Intellectual Property Protection (The EU is taking the most comprehensive approach). Furthermore, private sectors and policy makers are collaborating to develop rules to achieve a safe and ethical AI. And, the same is happening among different countries, which are pursuing international collaboration to understand and address the various risks[67].

In order to strike an appropriate balance between government oversight and innovation, it is essential for companies, policymakers and other stakeholders to participate in transparent and collaborative dialogue[68].

3.1 European Union – A risk based regulatory approach

There are many laws applicable to AI in Europe and, thanks to the *EU AI Act*[69] of 2024, the community is earning the record for being one of the first legislation systems providing a comprehensive legal framework for AI[70].

[67] *See* supra note 62.

[68] *Id.*

[69] *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (Artificial Intelligence Act), 2024 O.J. (L 2024/1689).

[70] *See* Timo Gaudszun et al., *AI Watch: Global regulatory tracker – European Union* (2025), WHITE & CASE, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-european-union.

Before talking about this hugely important framework, there is another regulation that is worth to be mentioned, the *GDPR*[71]. The EU *General Data Protection Regulation* (GDPR), enacted in 2016, focuses on data protection and privacy. Following it, organizations must safeguard personal data privacy, notify authorities of data breaches, ensure the transfer of data across borders and implement practices to remain compliant. It defines the requirement of explicit consent for the usage of personal data by AI models. So, following *GDPR*, AI developers must guarantee that consent is willingly provided, specific, informed and unequivocal. Even though, in some cases, AI can handle personal data based on the justified grounds of legitimate interest. Nevertheless, this definition requires careful balancing to ensure that the rights of data subject are fully protected and not undermined[72].

However, the *European Union's Artificial Intelligence Act*[73] (Regulation (EU) 2024/1689) is the pioneering legal framework in terms of Artificial Intelligence and is a model for all countries of the world[74]. It is the first comprehensive horizontal legal framework for AI regulation in EU[75]. And, while being an innovative document in the AI field, it follows and respects early European provisions, such as the *GDPR*[76].

It was proposed by the European Commission the 21st of April 2021 and it was definitively approved the 21st of May 2024 by the Council of the European Union[77]. It will become effective from the 2nd of August 2026, except some specific provisions[78].

Depending on its great advancement with respect to other Acts and other counties' regulations, it has the possibility to become a global standard or at least to have a great influence on the global directive

[71] *Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), 2016 O.J. (L119).

[72] *See* Exabeam, *The Intersection of GDPR and AI and 6 Compliance Best Practices,* EXABEAM, https://www.exabeam.com/explainers/gdpr-compliance/the-intersection-of-gdpr-and-ai-and-6-compliance-best-practices/#:~:text=GDPR%20defines%20the%20requirement%20for,grounds%20of%20“legitimate%20interest .

[73] *See supra note 69.*

[74] *See* Tania Goncalves, *The AI Act: Europe's Human Rights Contradiction Militarizing AI in the Name of Defense – The Human-Centric Illusion* (2025), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5158906 .

[75] *See supra note 70.*

[76] *See* Jon Chun et al., *Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US* (2024), ARXIV – CORNELL UNIVERSITY, https://arxiv.org/abs/2410.21279 .

[77] See European Council – Council of European Union, *Artificial Intelligence Act ,* COUNCIL OF EUROPEAN UNION, https://www.consilium.europa.eu/en/policies/artificial-intelligence/ .

[78] *See supra note 70.*

that will one day be approved[79]. Other Acts have already tried to take moves from it. For instance, immediately after its proposal, in late September 2021 Brazil's House of Representatives passed a Bill[80] (Which has now been rejected) to create a legal framework in terms of Artificial Intelligence[81]. The EU *AI Act* [82](“The Act”) aligns closely with the *Declaration on Digital Rights and Principles*[83], which indeed supports digital transformation in EU[84].

The *Act* adopts the definition of AI system from the *OECD*'s *AI principles*[85]. It says that an AI system is a: “Machine-based system that is designed top operate within varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments”[86].

Through the *Act* and the guidelines that it provides firms with, companies can ensure that AI systems respect individual rights, mitigate bias, promote inclusivity, enhance security and sustainability and, support freedom of choice. This approach both helps companies to meet regulatory requirements and empowers them to have an impact in the digital age, by encouraging the widespread adoption of AI[87].

The *AI Act* forms a part of a broader set of policy initiatives aimed at fostering AI development, including the *AI Innovation Package*[88], the establishment of AI factories[89] and the *Coordinated plan on AI*[90]. Collectively, these efforts promote safety, protect fundamental rights and encourage investment and innovation throughout the EU. Moreover, in order to facilitate the implementation of

[79] *See* Finextra, *What is the EU AI Act? Understanding Europe's first regulation on artificial intelligence* (2023), FINEXTRA, https://www.finextra.com/the-long-read/847/what-is-the-eu-ai-act-understanding-europes-first-regulation-on-artificial-intelligence .

[80] See Brazil's Chamber of Deputies, *Bill No. 21-A/2020 (2020),* DERECHOS DIGITALES, *https://www.derechosdigitales.org/wp-content/uploads/Brazil-Bill-Law-of-No-21-of-2020-EN.pdf* .

[81] *See* Melissa Heikkilä, *Brazil's AI law – US takes a risk-based approach – Social scoring* (2021), POLITICO, https://www.politico.eu/newsletter/ai-decoded/brazils-ai-law-us-takes-a-risk-based-approach-social-scoring/ .

[82] *See supra note 69.*

[83] *European Declaration on Digital Rights and Principles for the Digital Decade*, 2023/C 23/01 O.J. (C23) 1 (EU).

[84] *See* AI & Partners, *EU AI Act: Trustworthy AI for the Digital Decade* (2025), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5147156 .

[85] *See* OECD, *AI Principles*, OECD, https://www.oecd.org/en/topics/ai-principles.html .

[86] *See supra note 69.*

[87] *See supra note 84.*

[88] *See* Shaping Europe's digital future, *AI Innovation Package*, DIGITAL STRATEGY EU, https://digital-strategy.ec.europa.eu/en/factpages/ai-innovation-package .

[89] *See* Shaping Europe's digital future, *AI Factories*, DIGITAL STRATEGY EU, https://digital-strategy.ec.europa.eu/en/policies/ai-factories .

[90] *See* Shaping Europe's digital future, *Coordinated Plan on Artificial Intelligence*, DIGITAL STRATEGY EU, https://digital-strategy.ec.europa.eu/en/policies/plan-ai .

the *Act*, the European Commission has launched the *AI Pact*[91], which promotes its future implementation and engage with stakeholders[92].

The *AI Act* is a legal framework based on a risk-centered approach. It indeed classifies AI and the related regulation, basing on the level of risk attributed to the specific kinds of devices and uses[93].

The levels of risk in which the *Act* classifies AI are:

- Unacceptable risk: those AI devices are prohibited;
- High-risk: the main focus of the Act;
- Limited risk: systems subject to lighter transparency obligations (Chatbots and Deepfakes). Developers and deployers of them must ensure users' awareness of the interaction with AI (Rather than with a real person);
- Minimal risk: unregulated systems. They include the majority of AI applications available in EU, such as video games and spam filters. This is changing with Generative AI[94].

Furthermore, an AI system with civilian or law enforcement purposes, used for military, defense or national security scopes, should not fall within the scope of this Regulation, regardless of the type of entity carrying out those activities[95].

The obligations emerging from the *Act*, fall on deployers and developers of the systems (In particular, deployers have less obligations than developers), so to those that intend to place on the market or put into service those systems in the EU, regardless of whether they are based in the EU or in a third country. Also third country providers which produce devices used in EU have to respond to those obligations[96].

[91] *See* Shaping Europe's digital future, *AI Pact*, DIGITAL STRATEGY EU, https://digital-strategy.ec.europa.eu/en/policies/ai-pact .

[92] *See* European Commission, *AI Act,* SHAPING EUROPE'S DIGITAL FUTURE, *https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai* .

[93] *See* EU Artificial Intelligence Act, *High-level summary of the AI Act* (2024), EU ARTIFICIAL INTELLIGENCE ACT, https://artificialintelligenceact.eu/high-level-sum.mary/.

[94] *Id.*

[95] *See* EU Artificial Intelligence Act, *Recital 24*, EU ARTIFICIAL INTELLIGENCE ACT, https://artificialintelligenceact.eu/recital/24/#:~:text=An%20AI%20system%20placed%20on,entity%20carrying%20out%20those%20activities .

[96] *See supra note 93.*

Following the *Act*, all General Purpose AI (GPAI) model providers must provide technical documentation and instructions for use, by complying with the *Copyright directive*[97] and publishing summaries of the contents used for training. While, in the case that they present a systematic risk, they should conduct model evaluations and adversarial testing and, they should track and report serious incidents to ensure cybersecurity protections [98].

In order to enter more deeply in the classification of AI based on the level of risk, the first mention goes to the prohibited AI systems, analyzed in Chapter II, Art. 5[99]. The prohibited AI systems are distinguished by their unacceptable risk. They are those systems deploying subliminal, manipulative, or deceptive techniques, which distort behavior and impair informed decision-making, causing significant harm. They include AI devices exploiting vulnerabilities related to age, disability, or socio-economic circumstances which can distort behavior and cause harm. Also the biometric categorization systems are classified as such, so, those that infer sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation). However, those models are excluded when they provide labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorizes biometric data. Moreover, unacceptable risk is attributed to social scoring systems evaluating or classifying individuals or groups based on social behavior or personal traits and, to those systems assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits (except when they are used to augment human assessments based on objective, verifiable facts directly linked to criminal activity). They are prohibited also compiling facial recognition databases, which scrap untargeted facial images from the internet or CCTV footage and, systems inferring emotions in workplaces or educational institutions, except for medical or safety reasons. The last kind of unacceptable risk systems are 'Real-time'

[97] *Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC*, 2019 O.J. (L 130) 92.

[98] *See supra note 93.*

[99] *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (Artificial Intelligence Act), Chapter II Art. 5, 2024 O.J. (L 2024/1689).

remote biometric identification (RBI) in publicly accessible spaces for law enforcement. They are not allowed except when they are searching for missing persons, abduction victims or people who have been human trafficked or sexually exploited. Thus, when they prevent a threat to life, or a foreseeable terrorist attack, or they serve to identify suspects in serious crimes (such as murder, rape, armed robbery, narcotic and illegal weapons trafficking, organized crime, and environmental crime, etc.) hey are permitted[100].

RBI is only allowed when not using the tool would cause harm. For this reason, before using them the police must complete a fundamental rights impact assessment and register in the EU database (In justified cases of emergency the deployment can commence without registration, provided that it is registered later without delay). Also, before deployment, RBI must obtain authorization from a judicial authority or independent administrative authority (In justified cases of emergency, deployment can start without authorization, but it has to be requested within 24 hours. If then the authorization is rejected, deployment must cease immediately, deleting all data, results and outputs)[101].

The second and most important type of AI classified by the act is: High-risk AI, described in chapter III, Art. 6[102]. It includes those systems used as a safety component or a product covered by EU laws. They need to undergo a third-party conformity assessment under Annex I laws and under Annex III use cases (Non-banned biometrics, critical infrastructure, education and vocational training, employment, workers management and access to self-employment, access to and enjoyment of essential public and private services, law enforcement, migration, asylum and border control management, administration of justice, democratic processes and ethics). This requirement is abolished when the AI system performs a narrow procedural task, improves the result of a previously

[100] *See supra note 93.*

[101] *Id.*

[102] *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (Artificial Intelligence Act), Chapter III Art. 6, 2024 O.J. (L 2024/1689).

completed human activity, detects decision-making patterns or deviations from prior decision-making patterns, does not replace or influence the previously completed human assessment without proper human review, or if it performs a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III. If there is evidence that the AI system does not pose a significant risk to health, safety and fundamental rights or if it is needed to protect people, the Commission, through delegated acts, may modify or add these conditions. High-risk systems are also those that profile individuals. So, those that automate the processing of personal data to assess aspects of a person's life[103].

18 months after entry into force, the Commission will assess whether an AI system qualifies as high-risk, by referring to illustrative use cases. If a provider believes their AI system, even though being listed under Annex III, should not be categorized as high-risk, they must prepare and document a justification before placing it on the market or deploying it[104].

In Art. 8-17[105], the *Act* specifies the requirements for AI providers of high-risk systems. In particular they must establish a risk and quality management system to ensure compliance, they must also conduct data governance (to ensure that training, validation and testing datasets are relevant and free of errors) and draw up technical documentation to demonstrate compliance with the law. Providers have to design the high-risk system in a way that it automatically keeps the records of the events, allows humans oversight and achieves levels of accuracy, robustness and cybersecurity. Lastly, the systems must also come with instructions of use[106].

Furthermore, in Chapter V[107], the *AI Act* provides a clear definition for GPAI models. These are AI models characterized by a high-degree of generality, capable of effectively performing a broad variety

[103] *See supra note 93.*

[104] *Id.*

[105] *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (Artificial Intelligence Act), Art. 8-17, 2024 O.J. (L 2024/1689).

[106] *See supra note 93.*

[107] *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No*

of distinct tasks, regardless of how they are made available ne the market. This definition excludes AI models used solely for research, development, or prototyping prior to their release. All providers of GPAI models are required to prepare technical documentation (covering aspects such as training, testing and performance evaluation) and, must supply relevant information and documentation to downstream providers, aiming to incorporate the GPAI model into their own AI systems. Providers have also to establish a policy to respect the *Copyright Directive*[108] and publish a detailed summary about the content used for training the model. Models released under free and open licenses, with publicly accessible parameters, are only required to meet the last two obligations. While, providers of GPAI models with systemic risk (for which the cumulative amount of computer used for the training is greater than 10^25 floating points operations per seconds) have to notify whether their model enters in this classification within two weeks. They must perform model evaluations, assess and mitigate possible systematic risks, report serious incidents and, ensure adequate levels of cybersecurity protection. Until European harmonized standards are published, all GPAI model providers should demonstrate compliance with their obligations by following recognized Codes of Practice. Providers which do not adhere to them, must demonstrate alternative means of compliance for the Commission approval[109].

Furthermore, the *Act* provides for AI governance. In Chapter VI[110] indeed, it is stated that it will be established an AI Office, sitting within the Commission to monitor the effective implementation and compliance of GPAI model providers (Art. 64). It is given the AI Office the right to conduct evaluations on GPAI models, to assess compliance and to investigate systematic risks, following a qualified report from the scientific panel of independent experts (Art. 90)[111].

168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), Chapter V, 2024 O.J. (L 2024/1689).

[108] *See supra note 97.*

[109] *See supra note 93.*

[110] *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (Artificial Intelligence Act), Chapter VI , 2024 O.J. (L 2024/1689).

[111] *See supra note 93.*

This *Act* in its entirety claims to aim at reaching, within EU, AI systems that are: safe, traceable, transparent, environmentally friendly and non-discriminatory[112].

However, even though the *Act* has been globally accepted, it has received some critics.

Amnesty international for instance have criticized it for not completely banning real-time facial recognition, which they said, could damage human rights, civil space and rule of law in the European Union. It also criticized the absence of ban on exporting AI technologies that can harm human rights. Moreover, some startups argued that additional regulation would make European startups uncompetitive in comparison with American and Chinese ones. Also, La Quadrature Du Net (LQDN) described the *AI Act* as "tailor-made for the tech industry"[113] and, believes that self-regulation and exemptions in the *Act*, render it "largely incapable of standing in the way of the social, political and environmental damage linked to the proliferation of AI"[114] [115].

Building on these criticisms, numerous scholars have raised concerns about the Act's handling of secondary uses of trained AI models, which could have substantial effects on society. They believe that the *Act* can be misinterpreted and lead to not sufficiently supervised performances, depending on its narrow focus on deployment contexts and on its reliance on providers to self-declare intended purposes. Additionally, they criticize the *Act*'s great exemption of open-source models and its negligence in considering critical lifecycle phases, such as the reuse of trained models. So, they believe that it falls outside the scope of other regulations like the *GDPR*[116] [117].

[112] *See* European Parliament, *EU AI Act: first regulation on artificial intelligence* (2023), TOPICS EUROPEAN PARLIAMENT, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[113] *See* La Quadrature du Net, *WITH THE AI ACT ADOPTED, THE TECHNO-SOLUTIONIST GOLD-RUSH CAN CONTINUE* (2024), LA QUADRATURE DU NET, https://www.laquadrature.net/en/2024/05/22/with-the-ai-act-adopted-the-techno-solutionist-gold-rush-can-continue/ .

[114] Id.

[115] *See* Wikipedia, *Artificial Intelligence Act*, WIKIPEDIA, https://en.wikipedia.org/wiki/Artificial_Intelligence_Act#:~:text=On%2021%20April%202021%2C%20the,and%20Parliament%20concluded%20an%20agreement .

[116] *See supra note 71.*

[117] *See supra note 115.*

Furthermore, the expert Tânia Gonçlaves, in the paper "The AI Act: Europe's Human Rights Contradiction Militarizing AI in the Name of Defense – The Human Centric Illusion"[118] claims to believe that even though the EU *AI Act* was declared to be a pioneering legal framework balancing technological innovation and ethical constraints, a deeper scrutiny finds a fundamental contradiction. While the regulation claims to be human-centric, in reality its priorities the aligning with national security, law enforcement and military applications, rather than societal progress. By reading the *Act*, it indeed emerges that while civilian AI faces heavy regulatory scrutiny, military and security AI are almost exempted from regulation at all[119].

3.2 US Regulatory Framework – A fragmented, innovation-driven system

US, differently from European Union's *AI Act*[120], lack a comprehensive federal law specifically governing AI. Still, they have been established several executive orders, federal policies and practices related to AI governance, resulting in agency-specific regulations. In the United States indeed, AI governance is characterized by a decentralized approach. US law on AI focuses on sector-specific regulations and voluntary commitments from private companies. It strongly relies on guidance of the White House and of federal agencies such as the National Institute of Standards and Technology (NIST), which provide guidelines and standards to encourage self-regulation within the industry[121]. In the past congresses, the first federal laws on AI have been enacted as standalone legislation or as AI-related provisions and clauses of broader acts. Congresses work also on bipartisan framework, by overseeing AI-related issues through its bodies and by collaborating with federal agencies[122].

[118] *See* Tania Goncalves, *The AI Act: Europe's Human Rights Contradiction Militarizing AI in the Name of Defense – The Human-Centric Illusion* (2025), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5158906 .

[119] *Id.*

[120] *See supra note 69.*

[121] *See* Tatevik Davtyan, *The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained (*2024), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4954290 .

[122] *Id.*

Additionally, the various States have proposed and continue enacting AI laws. An important part of US approach is in fact that industries participate to the development of ethical guidelines, by collaborating with federal agencies. The main objectives of US AI policies are to foster openness and competitiveness in the AI economy and to enhance safety while managing risks[123].

Furthermore, currently, there is not an AI-specific regulator in the US. However, in 2023 the Federal Trade Commission, the Equal Employment Opportunity Commission, the Consumer Financial Protection Bureau and the Department of Justice issued a joint statement declaring themselves to be the authority that regulates software and algorithmic processes, including AI[124].

Nowadays, a great focus of discussion is the renewed Trump administration, which is partially reshaping the laws on AI introduced by the last president, Joe Biden[125].

Main legislations at the federal level concerning AI include some Acts that have been carried out in recent years. There can be cited, the *John S. McCain National Defense Authorization Act*[126] (NDAA) of 2019, which directed the Department of Defense to take part in AI initiatives, like appointing a coordinator. Since then, annual NDAAs have included AI-related defense, national security and intelligence provisions. Moreover, in 2020 it was enacted the *National Artificial Intelligence Initiative*[127] (NAII)(During President Trump's first mandate), which codified the American AI initiative, legalized the creation of National AI Initiative Office, formed an interagency committee at OSTP to coordinate AI programs, established a National AI Advisory Committee and directed AI activities across federal science agencies, such as NSF, NIST, NOAA and the Department of Energy[128]. This Act promotes and subsidizes AI innovation efforts across key federal agencies. It

[123] *See supra note 121.*

[124] *See* White & Case, *AI Watch: Global regulatory tracker – United States* (2025)*,* WHITE & CASE, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states .

[125] *See* Software Improvement Group, *AI Legislation in the US: A 2025 Overview* (2025), SOFTWARE IMPROVEMENT GROUP, https://www.softwareimprovementgroup.com/us-ai-legislation-overview/#:~:text=In%20the%20United%20States%2C%20the,Trump%20in%20his%20first%2Dterm .

[126] *John S. McCain National Defense Authorization Act for Fiscal Year 2019,* Pub. L. No. 115-232 (2018).

[127] *National Artificial Intelligence Initiative Act of 2020*, Pub. H.R. 6216 (2019-2020).

[128] *See supra note 121.*

focuses less on regulation of AI "per se" and more on fostering research and development in the field. It has the aim to establish the United States as a global leader in AI innovation[129].

Among other notable Acts, there can be identified: the *AI in Government Act*[130] of 2020, which created an AI Center of Excellence within the General Service Administration (GSA) and, the *Advancing American AI Act*[131] of 2022, which provided additional guidance for Federal Government's AI use. Under the latter, the Office of Management and Budget (OMB) was required to create guidance for AI use in federal agencies, to ensure AI contracts address privacy and civil rights and, to define an inventor in AI use cases[132].

Then, there can be highlighted some regulations that occupied of ruling the standards and limits that AI must adhere to. One of them is the *CHIPS and Science Act*[133]. It tasked agencies like the Department Of Energy (DOE), the National Institute of Standard and Technology (NIST) and the National Science Fund (NSF) with promoting AI R&D and creating standards for trustworthy AI. It can be noted also the *Countering Human Trafficking Act*[134], which required the Department of Homeless Security (DHS) to use AI and machine learning to develop systems to combat human trafficking. The *Algorithmic Accountability Act*[135] of 2024 is also worth to mention. It has the aim to regulate the use of automated decision systems (ADS), by requiring companies to conduct impact assessments for transparency, privacy, fairness and accuracy. Through this Act, large companies are required to conduct annual assessments to evaluate how their systems impact individuals[136].

Furthermore, by mid-2023, 94 bills were introduced in the 118th Congress. They focus on AI governance, federal training, political and disclosure restrictions on AI use in nuclear weapons and, decisions and biometric surveillance. In the same year, they were passed 2 house resolutions: the

[129] *See supra note 125.*
[130] *AI in Government Act of 2020*, H.R. 2575 (2019-2020).
[131] *Advancing American AI Act*, S.1353 (2021-2022).
[132] *See supra note 121.*
[133] *CHIPS and Science Act*, H.R. 4346 (2021-2022).
[134] *Countering Human Trafficking Act of 2021*, S. 2991 (2021-2022).
[135] *Algorithmic Accountability Act of 2023*, S. 2892 (2023-2024).
[136] *See supra note 121.*

House Resolution 66[137], urging the Congress to prioritize safe AI development, and the *House Resolution 3044*[138], about seeking transparency in AI use in political ads[139].

Then there are some relevant Bills for their contribute to AI privacy matters: the *Stop Spying Bosses Act*[140] of 2024, the *American Data Privacy and Protection Act*[141] of 2022, and the *SAFE DATA Act*[142] of 2022[143].

Moreover, in 2024 the US House of representatives published the *Bipartisan House Task Force Report on AI*[144], which provided guidelines for future AI advancements. It aims at protecting Americans from harmful or unintentional uses of AI and, suggests a risk-based approach to be established[145].

The last notable Act that is worth quoting is the *AI Research Innovation Accountability Act*[146] of 2024, calling for greater transparency, accountability and security in AI and, establishing a framework for AI innovation. This framework occupies of evaluating and testing high-risk AI systems and, requires companies that use them to produce transparency reports. It also empowers the National Institute of Standards and Technology to issue sector-specific recommendations[147].

In summary, the Congress should provide the structure and the resources for AI regulation by passing legislations and funding research. But, in practice, it has now refrained from enacting direct legislation for private sector AI use and, has invested heavily on AI research and development[148].

[137] *Expressing support for Congress to focus on artificial intelligence*, H. Res. 66 (2023-2024).

[138] *Amending House Resolution 211 to ensure that days occurring during the first session of the One Hundred Nineteenth Congress constitute calendar days for purposes of section 202 of the National Emergencies Act (50 U.S.C. 1622) with respect to a joint resolution terminating a national emergency declared by the President on February 1, 2025.* H. Res. 304 (2025-2026)

[139] *See supra note 121.*

[140] *Stop Spying Bosses Act*, S.262 (2023-2024).

[141] *American Data Privacy and Protection Act*, H.R. 8152 (2021-2022).

[142] *SAFE DATA Act*, S. 2499 (2021-2022).

[143] *See supra note 121.*

[144] *See* 118th Congress*, House Bipartisan Task Force on Artificial Intelligence Delivers Report (2024),* COMMITTEE ON SCIENCE SPACE AND TECHNOLOGY, *https://science.house.gov/2024/12/house-bipartisan-task-force-on-artificial-intelligence-delivers-report* .

[145] *See supra note 125.*

[146] *Artificial Intelligence Research, Innovation, and accountability Act of 2024*, S. 3312 (2023-2024).

[147] *See supra note 121.*

[148] *Id.*

The trust that the Government earns is fundamental. It is indeed always important to establish clear and responsible guidelines and policies that maximize AI benefits and minimize its risks. AI is changing quickly and, it is important for the evolving policies to always be updated. AI systems are influenced by the values of those who create them and, since US's policies have always aimed at transforming US into a global leader in AI and at reinforcing traditional American values, attracting emerging talents and investing in research are former actions that must be taken to stay competitive[149]. Furthermore, as aforementioned, since US legislation is fragmented and there is not a unique comprehensive act as in EU, some States have distinguished themselves by enacting their own Acts to regulate and foster the development of AI. One of them is Colorado[150].

On May 2024 the State of Colorado has enacted the *Colorado AI Act*[151], which will become effective in 2026. It is a framework that by borrowing several elements from the EU *AI Act*[152], has established the foundations for a comprehensive US AI Act. It adopts a risk-based approach, by targeting developers and deployers of high-risk AI systems. It requires developers to establish documentation around the purpose, intended uses, benefits and limitations of each system. So, high-level summaries of the data used for training must be disclosed, together with a record of the data governance measures adopted. Also, following the *Act*[153], developers must mitigate biases and provide proof of this, by also presenting documentation covering the purpose of each AI system, including benefits, intended applications, limitations and potential risks. They should establish procedures to mitigate against any identified risk and, provide instructions to deployers of high-risk AI systems on how to use and monitor them. Organizations must also adopt risk management policies and procedures that align with established industry guidelines, such as the *NIST AI Risk Management Framework*[154], or relevant ISO standards. The *Act* requires also the development of AI impact assessments and the

[149] *See supra note 125.*
[150] *Id.*
[151] *Consumer Protections for Artificial Intelligence Concerning consumer protections in interactions with artificial intelligence systems*, SB24-205 (2024).
[152] *See supra note 69.*
[153] *See supra note 151.*
[154] See NIST, *AI Risk Management Framework* (2023), NIST, https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook .

implementation of compliance indicators, to make sure that reasonable care was used to mitigate algorithmic discrimination when deploying high-risk AI systems[155]. This *Act* applies only to developers and deployers of high-risk systems in Colorado[156].

Another State that has considered enacting AI provisions is Illinois. On January 2025, the Illinois Supreme Court has published its *Artificial Intelligence Policy*[157], considering the recent advancements of Generative AI. Key guidelines for the integration of AI were established in judicial and legal systems, responsible and effective use was enhanced and, the integrity of court processes was safeguarded. Ethics and trust are always put at stand[158]. There is also a currently pending litigation in the AI context of the *Biometric Information Privacy Act*[159], providing for damages from the violations of privacy[160].

Another notable State that has enacted various Bills is California, in September 2024. The Bills passed concern matters such as election integrity, transparency, privacy, entertainment and government accountability. Some of the key laws include for instance the *Assembly Bill 2655*: *Defending Democracy from Deepfake Deception Act*[161]. It requires online platforms to identify and block the publication of materially deceptive content related to elections in California and, to label fake contents in general. There is also the *Assembly Bill 1836: Use of Likeness: Digital Replica Act*[162]. It establishes a cause of action for beneficiaries of deceased celebrities to recover damages for the unauthorized use of an AI-created digital replica of the celebrity in audiovisual works or sound recordings. The deployers of AI systems are required to obtain the consent of a deceased personality estate before producing or distributing the digital replica. Moreover, it may be pointed out the *Senate Bill 942:*

[155] *See supra note 125.*

[156] *See* White & Case, *AI Watch: Global regulatory tracker – United States,* WHITE & CASE, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states.

[157] See Illinois Supreme Court, *Illinois Supreme Court Announces Policy on Artificial Intelligence*, ILLINOIS COURTS, https://www.illinoiscourts.gov/News/1485/Illinois-Supreme-Court-Announces-Policy-on-Artificial-Intelligence/news-detail/ .

[158] *See supra note 125.*

[159] *740 ILCS 14*, (2008)

[160] *See supra note 156.*

[161] *Defending Democracy from Deepfake Deception Act of 2024* A.B. No. 261 (2024).

[162] *Use of Likeness: Digital Replica Act,* A.B. No. 1836 (2025).

California AI Transparency Act[163]. It mandates covered providers (AI systems publicly accessible within California with more than one million monthly visitors) to implement measures to disclose when a content has been generated or modified by AI. Another important Act was the *Bill 2013: Generative AI: Training Data Transparency Act*[164], which mandates developers of generative AI systems to publish a high-level summary of the datasets used to develop and train Generative AI systems. Lastly, it is worth mentioning the *California Privacy Protection Act*[165] (CPPA), regulating automated decision making[166] .

3.2.1 Regulatory Shifts in a Changing Political Climate

Nowadays, a matter that is completely changing the US Government structure and that is influencing the political and legislative landscape of AI is the recent Change of Presidency from the last President Joseph Robinette Biden Jr., to the current one, Donald John Trump[167].

In some respects, there has been a real shift from the previous policies to the new ones, some of the first has indeed been repealed. This text will try to explain all the measures taken by both presidencies to highlight the change of approach that has occurred.

The US White House has the role of leading federal agencies in interpreting and enforcing congressional laws, in order to shape regulatory decisions and prioritize particular issues. The first and most important Act of President Biden was the *Executive Order 14110* on the “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence”[168], adopted on October 2023. It had the aim of initiating a comprehensive government initiative to ensure responsible development and

[163] *California AI Transparency Act,* S.B. No. 942 (2023-2024)

[164] *Generative Artificial Intelligence: Training Data Transparency Act*, A.B. 2013 (2023-2024).

[165] *See California Consumer Privacy Act* (2024), ROB BONTA ATTORNEY GENERAL, HTTPS://OAG.CA.GOV/PRIVACY/CCPA .

[166] *See supra note 156*

[167] *See supra note 121.*

[168] *See* Joseph. R. Biden, Jr., *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), FEDERAL REGISTER, https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

deployment of AI[169]. It prioritized the elimination of risks. It focused on federal agencies and developers of foundation models by mandating the development of federal standards and, by requiring developers of the most powerful AI systems to share the safety tests results and other relevant information for US government [170]. It emphasized the federal agency leadership, industry regulation and collaboration with international partners. It outlined 8 main policy areas: safety and security, innovation and competition, worker support, AI bias and civil rights, consumer protection, privacy, federal use of AI and international leadership. It established the White House Artificial Intelligence Council, to guide AI governance. The document stressed the importance of disclosing details of AI systems, of the transparency that needs to be kept, of the anti-bias measures that have to be taken in AI systems, and of the responsible use of AI in the healthcare, communications and education sector needed. This way of using AI really enhanced the US global leadership. The *Executive Order 14110*[171] was built on previous administrations initiatives, such as the *AI Bill of Rights Blueprint*[172] and the NIST's *AI Risk Management Framework*[173][174]. The *White House Blueprint of an AI Bill of Rights*[175] is a document presented in October 2022, providing guidance for equitable access to AI systems. It bases on five principles helping to guide the design, use and deployment of automated systems. Those are: algorithmic discrimination and protection, data privacy, notice and explanation, human alternatives and, considerations and fallbacks[176]. This document reflects public concerns about the technologies' violation of civil and privacy rights[177].

One major issue that US faces is indeed the intersection of AI with Federal Law and copyright regulations. Issues of diversity, equity and inclusion are a great matter of concern nowadays.

[169] *See supra note 121.*
[170] *See supra note 156.*
[171] *See supra note 168.*
[172] *See* White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (2022), WH.GOV, https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/
[173] *See supra note 154.*
[174] *See supra note 95.*
[175] *See supra note 172.*
[176] *See supra note 156.*
[177] *See* Yannic Mahé, *Divergent Paths: Comparing AI Regulation in the US, EU, and China* (2024), LINKEDIN, https://www.linkedin.com/pulse/divergent-paths-comparing-ai-regulation-us-eu-china-yannick-mahé-ztlre/ .

Companies like Microsoft and Amazon have faced great criticism for AI systems replicating discriminatory patterns. For instance, Amazon scrapped its AI recruiting tool in 2018 after discovering it was biased against women. Without effective governance and oversight, such algorithms can inadvertently contribute to societal divisions, misinformation campaigns and even political manipulation. The introduction of *AI Bill of Rights*[178] in October 2022 aimed to ensure fairness, inclusivity and accountability in AI systems[179].

The Obama administration had laid the foundation for US comprehensive federal AI policy in the Report: "Preparing for the Future of Artificial Intelligence"[180] (2016), published by the National Science and Technology Council (NSTC). It addressed the challenges and opportunities of AI, by emphasizing ethical considerations, regulatory challenges and national security[181].

Because of the importance of the *EO 14110*[182], many initiatives were taken. In March 2024 for instance, it was issued the *AI Accountability Policy Report*[183] by the National Telecommunications and Information Administration (NTIA), emphasizing the need for accountability in AI systems as they become more integrated into daily life[184].

However, this *EO* was strongly criticized by Republicans, who were accusing it of being too prescriptive and anti-innovation. They took for example the invocation by the Order of the *Defense Production Act*[185] (DPA), which requires companies developing AI foundation models that pose risks to national security and economy, to share results of the safety tests[186]. In the same period, it was published by the Office of Management and Budget (OMB) the policy *Advancing Governance,*

[178] *See supra note 172.*

[179] *See supra note 177.*

[180] See Executive Office of the President National Science and Technology Council Committee on Technology, *Preparing for the Future of Artificial Intelligence* (2016), OBAMA WHITE HOUSE, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf .

[181] *See supra note 121.*

[182] *See supra note 168.*

[183] See *AI Accountability Policy Repor*t (2024), NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report .

[184] *See supra note 121.*

[185] *Defense Production Act*, Pub. L. 81-774 (1950).

[186] *See* Ken D. Kumayama et al., *US Federal Regulation of AI Is Likely To Be Lighter, but States May Fill the Void* (2025), SKADDEN, https://www.skadden.com/insights/publications/2025/01/2025-insights-sections/revisiting-regulations-and-policies/us-federal-regulation-of-ai-is-likely-to-be-lighter .

Innovation, and Risk Management for Agency Use of AI[187], aiming at guiding federal agencies in promoting AI governance and innovation while addressing public rights and safety risks. Moreover, the US Department of the Treasury, in March 2024, released a report about: "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector"[188], by highlighting several issues, such as the growing capability gap between large and small institutions, data storages for anti-fraud AI models, and better regulatory coordination. In order to focus on AI-related operational risks, cybersecurity and fraud prevention, the Treasury plans to work with the private sector, regulators and international partners[189].

Furthermore, the Biden administration, demonstrated its interest in the development of trustworthy AI in July 2023, by securing voluntary commitments from major AI companies such as Amazon, Google, Meta and Microsoft, to enhance AI safety, security and transparency. These companies agreed to rigorous testing, sharing safety protocols, reporting vulnerabilities and developing tools to identify AI-generated content, by also addressing societal impacts like bias, privacy, climate change and healthcare[190].

When President Trump took office on January 2025 instead, many of the efforts made by Biden administration were revoked. Orders like the *Executive Order 14141*[191] (Biden's 2025 *AI Infrastructure EO*) and the *Executive Order 14144*[192] (Biden's 2025 *Cybersecurity EO*) remain in force, but Trump started to take off many policies and Executive Orders to revolutionize the system in use[193].

[187] *See* Executive Office of the President Office of Management and Budget, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (2024), WHITE HOUSE, https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf .

[188] *See* U.S. Department of the Treasury, *Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector* (2024), HOME TREASURY, https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf .

[189] *See supra note 121.*

[190] *Id.*

[191] *See* Joseph R. Biden, Jr., *Executive Order 14141—Advancing United States Leadership in Artificial Intelligence Infrastructure* (2025), THE AMERICAN PRESIDENCY PROJECT, *https://www.presidency.ucsb.edu/documents/executive-order-14141-advancing-united-states-leadership-artificial-intelligence*

[192] *See* Joseph R. Biden, Jr., *Executive Order- 14144-Strenghtening and promoting innovation in the Nation's cybersecurity* (2025), FEDERAL REGISTER, https://public-inspection.federalregister.gov/2025-01470.pdf

[193] *See supra note 125.*

First of all, on January 20th, 2025, the President Trump, revoked Biden's *EO 14110*[194]. He indeed had already announced his intensions at the Republican National Convention in July 2024, by stating: " We will repeal Joe Biden's dangerous Executive Order that hinders AI innovation and imposes radical left-wing ideas on the development of this technology. In its place, Republicans support AI development rooted in free speech and human flourishing"[195].

Trump promotes a freer policy in terms of AI. He pushes for a more hands-off, free market oriented political philosophy in order to reach a leading position in the global governance on AI. Indeed on January 23rd 2025, he signed the *Executive Order* titled: "Removing Barriers To American Leadership in Artificial Intelligence"[196]. This policy serves primarily to enhance America's global AI dominance and, to promote human flourishing, economic competitiveness and national security. AI systems developed must indeed be free from ideological bias or engineered social agendas. Within 180 days of this order, key advisors of science, technology, AI, crypto, national security, economic policy, and domestic policy, along with relevant government officials, must create and submit the President a plan to carry out the policy. Furthermore, key officials including APST, the Special Advisor for AI and Crypto and the APNSA must review all action taken under the old Biden's *Executive Order 14110*[197] and identify those that conflict with the new policy, in order to revise or rescind them[198].

All the orders administered by Trump focus on a reduced regulatory oversight, which lets the AI development foster. He had already announced this pattern at the end of his first mandate with the memo: "Guidance for Regulation of Artificial Intelligence Applications"[199] in 2020. It advocated for

[194] *See supra note 168.*
[195] *See supra note 125.*
[196] *See* Donald J. Trump, *Removing Barriers to American Leadership in Artificial Intelligence* (2025), THE WHITE HOUSE, https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/
[197] *See supra note 168.*
[198] *See supra note 125.*
[199] *See* Department of Health and Human Services, *Guidance for Regulation of Artificial Intelligence Applications* (2020) , https://www.hhs.gov/sites/default/files/department-of-health-and-human-services-omb-m-21-06.pdf .

an innovation-friendly approach to AI, which avoided particular regulatory or non-regulatory actions hampering AI growth[200].

For this, in his current mandate, it can be seen for instance that AI infrastructure investments are prioritized. The recent Stargate Project with OpenAI for example. Military AI development will be pursued by Trump, who will initiate a "Manhattan Project style" for AI in defense[201].

The political scenario in US is currently changing a lot, with new updates every day, and only time will tell how AI legislation will develop under current administration[202].

The problem is that, as Squire Patton Boogs' professional Mattew Kirk suggest, Trump's EO may widen the gap between Federal and State AI regulatory regimes. Indeed, while Trump's *Order* signals a federal shift toward prioritizing innovation by reducing regulatory constraints, States like Colorado, California and Texas have already enacted AI laws with varying scopes and degrees of oversight. Growing state involvement in AI-related activities could result in greater regulatory fragmentation, with individual states introducing their own rules to address issues such as high-risk AI applications, transparency, and sector-specific oversight[203].

Moreover, if the Congress enacts an AI law that prioritizes innovation over risk-mitigation, stricter state regulations could face federal preemption. Until then, organizations must closely monitor both federal and State developments to navigate this evolving and increasingly fragmented AI regulatory landscape[204].

However, the new imposition of tariffs by the US President, is likely to increase all the costs related to the construction of AI technologies such as construction materials, computer parts, cooling infrastructure and power supplies, by damaging US lead on AI. The costs could be so high that

[200] *See* Ken D. Kumayama et al., *US Federal Regulation of AI Is Likely To Be Lighter, but States May Fill the Void* (2025), SKADDEN, https://www.skadden.com/insights/publications/2025/01/2025-insights-sections/revisiting-regulations-and-policies/us-federal-regulation-of-ai-is-likely-to-be-lighter..

[201] See supra note 125.

[202] *Id.*

[203] *See* Mattew Kirk et al., *Key Insights on President Trump's New AI Executive Order and Policy % Regulatory Implications* (2025), SQUIRE PATTON BOGGS, https://www.squirepattonboggs.com/en/insights/publications/2025/02/key-insights-on-president-trumps-new-ai-executive-order-and-policy-regulatory-implications .

[204] *Id.*

companies might need to consider building datacenters abroad. Says Chris Miller, author of "Chip War"[205] that the increased costs of datacenter construction create a real risk that the US might begin losing grounds to China in the AI race[206]. The short-term impact will be significant, and the long-term impact is unclear[207].

Still, a recent research published by Epoch AI[208] shows that the costs of using AI are falling at an high speed in recent years. In short, in a year from now, using a certain model will require a lot less computing power and therefore money, so even though Trump's tariffs will add costs to datacenter components, researchers believe that AI usage is likely to get cheaper anyway[209].

3.3 China & Russia – AI as a state-controlled technology

Russia and China have similar approaches to AI policy at the State Level. Their initiatives may be a valid alternative to the Western model of AI development. In their view, the State plays a significant role, by coordinating private businesses and stimulating their development. The priorities of Russia and China in the field of digital sovereignty largely coincide, together with fields like the internet, investments in data centers and development of their own social platforms and technologies. Furthermore, their alternatives to Western countries have proved to be successful. Russian Vkontakte for instance is very popular in Central Asia and, the Chinese platform WeChat is a serious competitor of American Social Networks[210].

[205] *See* Chris Miller, *Chip War: the fight for the world's most critical ideology* (2022).

[206] *See* Billy Perrigo, *How Trump's Tariffs Could Make AI Development More Expensive*, 2025 TIME 1.

[207] *See* Epoch AI, *LLM Inference prices have fallen rapidly but unequally across tasks (*2025), EPOCH AI, https://epoch.ai/data-insights/llm-inference-price-trends .

[208] *Id.*

[209] *See supra note 206.*

[210] *See* Anna Sytnik, *Russia and China: Development of Artificial Intelligence in Eurasia* (2025), VALDAI DISCUSSION CLUB, https://valdaiclub.com/a/highlights/development-of-artificial-intelligence-in-eurasia/ .

Still, a large amount of data is needed to train AI systems successfully. So, it is often mentioned that the two countries could join efforts in collecting and labelling data, taking into account the specifics of cultures and languages[211].

On January 2025, the Russian President Vladimir Putin instructed the Government and Sberbank, the country's largest bank and tech innovator, to team up with China to develop AI[212].

Putin's instructions were published on Kremlin's website three weeks after his announcement that Russia would team up with BRICS partners and other countries to develop AI. Indeed, the sanctions imposed by Western countries to Russia for its war against Ukraine, penalized a lot the country, which in turn had to establish other alliances[213].

In December 2024 in Moscow there was an International Conference on AI, where Putin emphasized the necessity to develop AI technology. For this purpose, the President signed a list of orders about the implementation of it into government systems and, about the development of AI education and training. A platform was established in Moscow to showcase achievements in AI technology[214].

Also China agrees by its part. Specifically, Liu Wei, director of human Machine interaction and cognitive engineering laboratory in Beijing, believes and told Global Times that the potential of a Russia-China cooperation would be immense. Both sides could benefit by this alliance, to strengthen areas like finance, manufacturing, transportation and computing. China's application capabilities, data resources and technological foundation could really provide practical application scenarios to Russia's theoretical research. While Russia's advantages in AI algorithms and theories could help China achieve deeper breakthroughs in AI research[215].

On February 2025, Russian Chinese consultations on the military use of AI technologies, were entertained in Beijing. They discussed the similar attitudes of the two countries towards initiatives

[211] *Id.*

[212] *See* Kaspersky AI Security Team, *AI Regulation in Russia* (2024), KASPERSKY, https://ai-cert.kaspersky.com/ai-regulation-ru.html#:~:text=AI%20regulation%20in%20Russia%20at,of%20the%20Russian%20Federation%20No .

[213] *See Development of AI regulations in Russia*, 2025 CBJ 5.

[214] *See supra note 212.*

[215] *See Development of AI regulations in Russia*, 2025 CBJ 3,4.

related to the AI use for military purposes and, great attention was given to the coordination of actions within the Group of Governmental experts of the States Parties to the convention on Certain Conventional Weapons on Lethal Autonomous Weapons Systems[216].

Russia's attempts to secure China's support in advancing Artificial Intelligence are seen as a significant challenge to the US' leadership in the field. "The Russian president sees his country in global competition for AI with the United States and has positioned the state resources to try and compete with the U.S. in information and cyberspace – two areas where artificial intelligence is supposed to aid Russia in what they see as Western narratives and influence"[217] said Samuel Bendett, adjunct senior fellow at the Center for a New American Security. Moscow sees Beijing's success in AI as an example to follow and believes that its cooperation with China is fundamental for acquiring artificial intelligence-related skill sets, knowledge and technology. Western sanctions imposed on Russia since its invasion of Ukraine in 2022 have limited the country's AI development and, Moscow has turned to Beijing to offset the restriction. Sberbank, which Putin instructed to collaborate with China, is under Western sanctions. It is Russia's largest bank and is really enhancing the country's AI development efforts[218].

But the bank's first deputy CEO, Alexander Vedyakhin is positive. In December 2024, he claimed to believe that, despite Western sanctions, Russia can improve its AI ranking by 2030 through its own development[219].

Sam Bresnick, research fellow at Georgetown University's Center for Security and Emerging Technology, notes that it remains uncertain how Beijing would stand to gain from assisting Moscow in AI development. China might want some military technologies and wartime data from Russia in return[220]. Moreover, James Lewis, director of the Strategic Technologies Program at the Center for

[216] *See Development of AI regulations in Russia*, 2025 CBJ 6.

[217] *See* Christy Lee, VOA, *Russia turns to China to step up AI race against US* (2025), VOA, https://www.voanews.com/a/russia-turns-to-china-to-step-up-ai-race-against-us/7931829.html .

[218] *Id.*

[219] *Id.*

[220] *Id.*

Strategic and International Studies, said that Russia is likely to use AI technology in enhancing drones as well as in making weapons, with improved target detection and attack speed. Indeed, Lewis believes that the China-Russia AI partnership would create new risks for the US[221].

3.3.1 Russia

The regulatory environment for Artificial Intelligence in Russia is still evolving and reflects the country's strategic priorities in technology, security, and sovereignty. The Russian government has recognized AI as a key driver of economic growth and technological advancement, but, its approach to regulation emphasizes control, national security and ethical considerations. The legal landscape for AI in Russia is shaped by a combination of national strategies, specific laws, ethical frameworks and Experimental Legal Regimes[222]. The country is currently trying to develop legal framework to regulate Artificial Intelligence. Experts believe that it does not need an immediate comprehensive legislation, but it would be sufficient to focus on fixing ethical and technical standards[223].

Regulation of AI is carried out by the President of the Russian Federation[224]. In addition to his instructions, AI in Russia is regulated by resolutions and orders of the Government of the Russian Federation and of the Ministry of Transportation of the Russian Federation[225].

The dominant law in terms of AI in Russia, is the *Federal Law of July 2020, No. 258-FZ* "On Experimental Legal Regimes in the Sphere of Digital Innovations in the Russian Federation"[226], which came into force in 2021. Pursuant to its provisions, people involved in the development and implementation of digital innovations (Experimental Legal Regimes) are given the opportunity to

[221] *Id.*
[222] *See supra note 217.*
[223] *See supra note 215.*
[224] *See* Anton Vasiliev et al., *Ethical and legal aspects of the use of artificial intelligence in Russia, EU, and the USA: comparative legal analysis 2019 Redalyc 16.*
[225] *See* Альянс в сфере искусственного интеллекта, *A Commission on AI Ethics has been established in Russia* (2022), https://a-ai.ru/?page_id=1699&lang=en#:~:text=It%20was%20created%20at%20the,work%20together%20to%20implement%20it.
[226] *Federal Law of the Russian Federation*, 2021, No. 258-FZ.

implement their practical applications by removing the restrictions established by regulatory legal acts called sandboxes. Thus, these modes will allow businesses to reduce times and costs for the development, testing and implementation of new technologies, as well as reducing legal risks[227]. It supports the development of digital medical technologies, highly automated vehicles and new technologies for the financial market, sales of products and, architectural and construction design[228]. Moreover, pursuant to *Resolution of the Government of the Russian Federation No. 1618* dated October 7, 2020, "On Amending Clause 1 of the Regulation on the Ministry of Economic Development of the Russian Federation"[229], the Ministry of Economic Development of Russia is determined as an authorized federal executive body ensuring the normative legal regulation and the executing the powers provided for by *Federal Law No. 258*[230] (2020). This Law on Experimental Legal Regimes in the field of digital innovations in the Russian Federation[231] focuses on creating experimental legal regimes (ERLs) or regulatory sandboxes, in order to allow the implementation of innovations in test mode, with the exception of the direction of development, testing and implementation of digital innovations pointed out by specified Federal Law[232].

2020 was also the year in which the Russian government approved the *Concept for the Regulation of AI and Robotics*[233], in order to develop the technology and respect the rights of citizens to ensure the safety of the state, of the society and of the individuals[234].

Russia until now has undertaken many initiatives and provisions to address AI development. The cornerstone has been the "National Strategy for the Development of Artificial Intelligence until 2030"

[227] *See* Oksana Mamima et al., *Experimental legal regimes for digital innovation and a special regulation mechanism: new concepts of russian legislation and first projects* (2021), SHS WEB OF CONFERENCES, https://www.shs-conferences.org/articles/shsconf/pdf/2021/17/shsconf_mtde2021_02009.pdf.

[228] *See* Stip Compass, *Federal Law "On Experimental Legal Regimes in the Field of Digital Innovation in Russia"* , STIP OECD, https://stip.oecd.org/stip/covid-portal/policy-initiatives/covid%2Fdata%2FpolicyInitiatives%2F944 .

[229] *Resolution of the Government of Russian Federation*, 2020, No. 1618.

[230] *See supra note 226.*

[231] *See* Gary E.Murphy et al., *Russia Adopts Law on Regulatory Sandboxes* (2020), DEBEVOISE & PLIMPTION, https://www.debevoise.com/insights/publications/2020/09/russia-adopts-law-on-regulatory-sandboxes .

[232] *See supra note 227.*

[233] *See Concept for the Regulation of Artificial Intelligence and Robotics,* ICT MOSCOW, *https://ict.moscow/en/news/concept-for-the-regulation-of-artificial-intelligence-and-robotics-until-2024-has-been-approved/*

[234] *See supra note 225.*

(2019)[235]. It outlines the goals and key tasks for AI development in the Russian Federation and, ensures that its applications will be destinated to achieve national interests and strategic national priorities. It addresses matters such as Protection of Human rights and freedom, safety of AI systems, transparency and security and, is not mandatory for AI developers themselves, but it provides a set of recommendations aimed at promoting ethical and safe AI systems[236].

Furthermore, in Russia, there is no intellectual property regulation to protect AI generated contents. However, if an author while using AI only as a tool has given a creative contribution to a work, the resulting content may be protected by copyright. Even though, AI systems are trained with large datasets, so it may be possible for it to either generate results that reproduce fully or partially a user or, to emulate the style of a real author. While the second case falls outside the IP regulation, the first one may be illegal and may lead to liability for the right holder even in cases of partial reproduction[237].

Moreover, in 2022, an extraterritorial provision was added to Russia Data Protection Law, which states that collecting data from Russian citizens is allowed only if there is a contract or consent. AI systems may be used to analyze voices or images of individuals and, in some cases, they can be classified as biometric personal data by being subject to stricter controls. These data must be carried out using databases located in Russia. Transferring data abroad would need compliance with special requirements, such as assessing the recipient and notify the competent authority. The law prohibits to make decisions that have legal consequences only basing on automated processing of personal data without written consent[238].

In the same year (2022), it was established a Commission on AI Ethics in Russia. It is a body for the development of ethical regulation of AI technologies. It occupies of developing a methodology to

[235] *See Decree of the President of the Russian Federation On the Development of Artificial Intelligence in the Russian Federation,* (2019), CSET, https://cset.georgetown.edu/wp-content/uploads/Decree-of-the-President-of-the-Russian-Federation-on-the-Development-of-Artificial-Intelligence-in-the-Russian-Federation-.pdf .

[236] *See supra note 225*

[237] *See supra note 215.*

[238] *Id.*

assess the risks and the humanitarian impact of AI systems and of creating criteria to assess the compliance with the Code[239].

In matter of advertising instead, AI is allowed to create it and, its distribution must comply with Federal Law "On advertising"[240]. In particular, it must be inter alia truthful, fair, complete and ethical[241].

On May 2024 then, thanks to the Ministry of Digital Development, Communications and Mass Media of the Russia Federation, a consortium was established to research AI technology security[242].

Furthermore, in January 2025, it entered in force the *Bill establishing Digital Innovation and AI in Experimental Legal Regimes* (Bill No. 512628-8)[243]. It was passed by the State Duma in 2024 and aims at broadening the scope of responsibility damages incurred during the digital innovation testing. It nominates a Commission addressing the damages of AI and, provides mechanisms for tracking and identifying individuals responsible for AI-related incidents. The Bill tries to make the process of developing digital innovation more efficient, by eliminating requirements such as the absence of a criminal record for initiators and extending the validity periods of these regimes[244].

In conclusion, Russia's approach focuses mainly on those areas of application where strict regulation is considered critically necessary[245].

According to the BRICS Competition Law & Policy Centre, Russia's updated Artificial Intelligence framework will enter in force in 2025 and, will prohibit AI technologies to be used for education purposes unless they foster student's development. It will also address matters such as the role of

[239] *See supra note 225.*

[240] *Federal Law On Advertising*, 38-FZ (2025).

[241] *See supra note 215.*

[242] *See supra note 225.*

[243] Postanovleniia palat Federal'nogo Sobraniia [resolution of the State Duma] 2024, Bill No. 512628-8.

[244] *See* Digital Policy Alert, *Russia: Passed Bill establishing Digital Innovation and AI in Experimental Legal Regimes(Bill No. 512628-8)* (2024), DIGITAL POLICY ALERT, https://digitalpolicyalert.org/event/21208-passed-bill-establishing-digital-innovation-and-ai-in-experimental-legal-regimes-bill-no-512628-8 .

[245] *See supra note 225.*

neural networks in healthcare, the responsibility for AI-generated creative works and accountability for harm caused by AI systems[246].

3.3.2 China

Thanks to its rapid advancements in Artificial Intelligence (AI), China has earned the position of being one of the global leaders in AI technology. The Chinese government has established a comprehensive regulatory framework that addresses both the opportunities and risks associated with AI, aiming to encourage innovation while retaining tight oversight of its development[247].

China has implemented numerous regulations to obtain a balance between innovation and social control, by focusing for example on recommendation algorithms for disseminating content, deep synthesis technology and generative AI[248].

Chinese AI legal framework is characterized by strong complexity, agility, stability and flexibility and, provides incentives for both public and private entities, together with administrative actions to mitigate AI risks[249]. The 20th National Congress of the Communist Party of China, positions AI as a strategically vital technology for the country's economic modernization and global competitiveness[250].

China's regulatory approach to AI reveals a dual strategy, which promotes innovation while ensuring tight control[251]. It is indeed strongly influenced by China's political background as an authoritarian

[246] *See* BRICS Competition- Law & Policy Centre, *RUSSIAN AUTHORITIES UNVEIL UPDATED AI REGULATION FRAMEWORK*(2024), BRICS COMPETITION, https://www.bricscompetition.org/news/russian-authorities-unveil-updated-ai-regulation-framework#:~:text=Russia's%20updated%20artificial%20intelligence%20(AI,rather%20than%20foster%20their%20development.

[247] *See* 360 Business Law, *China's Approach to AI Regulation* (2025), 360 BUSINESS LAW, https://www.360businesslaw.com/blog/chinas-approach-to-ai-regulation/#:~:text=China's%20regulatory%20approach%20to%20AI%20demonstrates%20a%20dual%20strategy%3A%20promoting,ensure%20alignment%20with%20national%20interests.

[248] See Baiyand Xiao, *Agile and Iterative Governance: China's Regulatory Response to Ai* (2024), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4705898 .

[249] *Id.*

[250] *See* Wayne Wei Wang, *Artificial Intelligence "Law(s)" in China: Retrospect and Prospect* (2025), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5039316 .

[251] *See supra note 247.*

regime which follows communist principles and aims at a society organized with collective ownership of resources and state-controlled production [252]. The key features of this strategy include strong governmental oversight, so that AI companies must submit their algorithms and AI generated contents for government review (to ensure alignment with national interests and ethical and political standards) and, educational initiatives, in order to build a workforce proficient in AI technologies. Moreover, the aforementioned dual strategy includes the control of misinformation. So, measures to detect and prevent the spread of AI generated misinformation, particularly in sectors like finance, which are prone to manipulation[253].

Since 2017, prominent domestic corporations including Baidu, Huawei, Tencent, and Alibaba have been designated by central authorities as 'national AI champions'. They were entrusted with not only pioneering AI research, development and applications, but also with fostering data sharing, distributing open-source software and enhancing the overall AI ecosystem[254].

Anyway, in China, the advanced technological infrastructures and their pro-innovation policies have allowed corporations to become global. Even if China falls behind US in fundamental AI regulations, its open innovation environment will probably attract investors in the long run. Indeed, commentators believe that Chinese firms might have an edge over US and Europe because of the less restrictive regulatory environment, which offers domestic tech companies major opportunities to innovate[255].

China's legal hierarchy consists of five tiers in a descending order of authority. The first one includes National People's Congress-level laws[256], such as the *Next Generation AI development Plan* [257] and

[252] *See* Jinghan Zeng, *Artificial and China's authoritarian governance* (2020), RESEARCHGATE, https://www.researchgate.net/publication/344678370_Artificial_intelligence_and_China's_authoritarian_governance .

[253] *See supra note 247.*

[254] *See supra note 248.*

[255] *Id.*

[256] *See supra note 250.*

[257] *See* State Council of China, *Next Generation Artificial Intelligence Development Plan* (2017), CHINA AEROSPACE STUDIES INSTITUTE, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-03-02%20China%27s%20New%20Generation%20Artificial%20Intelligence%20Development%20Plan-%202017.pdf .

the *Principles of Governance for the Next Generation AI-Developing Responsible AI*[258] [259]. Then there are Administrative regulations[260], such as the *Algorithmic Recommendation Regulation*[261], the *Deep Synthesis Regulation*[262], Interim Measures[263] like the *Generative AI Regulation*[264] and *Trial Measures for Ethical Review of Science and Technology*[265] [266]. The third layer consists of Departmental and local regulations[267], so measures like the *Shanghai New Generation AI Algorithm Innovation Action Plan 2021-2023*[268], *Shanghai Regulations on Promoting the Development of AI*[269] and *Shenzhen Regulations on Promoting the Development of AI*[270] [271]. Then there are Normative instruments[272], so laws in the *Civil Code*[273], such as the *Personal Information Protection Law*[274], the *Data Security Law*[275], the *Cybersecurity Law*[276], the *E-Commerce Law*[277] and the *Copyright Law*[278]

[258] See National Governance Committee for the New Generation Artificial Intelligence, *Governance Principles for the New Generation Artificial Intelligence--Developing Responsible Artificial Intelligence* (2019), CHINADAILY, *https://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html*

[259] *See supra note 248.*

[260] *See supra note 250.*

[261] *See* Cyberspace Admin. of China, *Internet Information Service Algorithmic Recommendation Management Provisions* (2022), https://www.cac.gov.cn/2021-12/31/c_1642894602930410.html

[262] See Provisions on the Administration of Deep Synthesis of Internet Information Services (深度合成管理规定), CHINA LAW TRANSLATE, https://www.chinalawtranslate.com/en/deep-synthesis/ .

[263] See *Interim Measures for the Management of Generative Artificial Intelligence Services* (2023) CHINA LAW TRANSLATE, https://www.chinalawtranslate.com/en/generative-ai-interim/

[264] *See supra note 248.*

[265] See China Briefing, *Ethical Review of Science and Technology in China: Draft Trial Measures* (2023), https://www.china-briefing.com/news/china-ethical-review-of-science-and-technology-draft-trial-measures/ .

[266] *See supra note 248.*

[267] *See supra note 250.*

[268] Shanghai New Generation AI Algorithm Innovation Action Plan (2021–2023), Shanghai Municipal People's Government, 2021.

[269] *Regulations of Shanghai Municipality on Promoting the Development of the Artificial Intelligence Sector*, 2022.

[270] *Regulations of Shenzhen Special Economic Zone on Promoting the Artificial Intelligence Industry*, 2022.

[271] *See supra note 248.*

[272] *See supra note 250.*

[273] *Zhonghua Renmin Gongheguo Minfa Dian* (中华人民共和国民法典) [Civil Code of the People's Republic of China], art. 1 (promulgated by the Standing Comm. Nat'l People's Cong., 2021).

[274] *Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa* (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China], art. 1 (adopted by the Standing Comm. Nat'l People's Cong., 2021).

[275] *Zhonghua Renmin Gongheguo Shuju Anquan Fa* (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China], art. 1 (adopted by the Standing Comm. Nat'l People's Cong., 2021).

[276] *Zhonghua Renmin Gongheguo Wangluo Anquan Fa* (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China], art. 1 (adopted by the Standing Comm. Nat'l People's Cong., 2017).

[277] *Zhonghua Renmin Gongheguo Dianzi Shangwu Fa* (中华人民共和国电子商务法) [E-Commerce Law of the People's Republic of China], art. 1 (adopted by the Standing Comm. Nat'l People's Cong., 2019).

[278] *Zhonghua Renmin Gongheguo Zhuzuoquan Fa* (中华人民共和国著作权法) [Copyright Law of the People's Republic of China], art. 1 (adopted by the Standing Comm. Nat'l People's Cong., 1991).

[279]. And lastly, there have to be quoted the technical standards[280], such as the *Guidelines for Personal information security specification*[281], the *AI-Technical Specification for Deep Synthetic Image system*[282], the *Prevention of Ethical Security Risks of AI*[283], the *Security Specification and Assessment Methods for Machine Learning Algorithms*[284] and the *Guidance for Personal Information Security Impact Assessment*[285]. However, details on how AI will be governed are sparse in these policies and a unified law for AI governance is absent[286].

An important institution in the Chinese government able to issue regulations, is the Cyberspace Administration of China (CAC)[287] . It is the lead regulator for Generative AI technology and has the authority to conduct security assessments, supervisory inspections, and impose penalties for any violation in accordance with relevant laws and regulations[288]. Some of its provisions address Recommendation Algorithms, Deep synthesis (Deepfake) Algorithms and Generative AI. The providers of these technologies, before offering services in China, must register detailed information with the CAC[289].

Furthermore, in China, numerous cities like Shanghai, Shenzhen and Beijing have organized themselves to enact AI-specific local regulations. Shanghai's and Shenzhen's regulations aim to promote the development of various types of AI, while Beijing focuses on promoting autonomous

[279] *See supra note 248.*
[280] *See supra note 250.*
[281] *Guojia Guifan 个人信息安全规范* [Guidelines for Personal Information Security Specification], GB/T 35273-2020 (issued by Standardization Administration of China, 2020).
[282] *See* China Translate, *Measures for Labeling of AI-Generated Synthetic Content* (2025), https://www.chinalawtranslate.com/en/ai-labeling/ .
[283] *Guójiā Guīfàn 个人信息安全规范* [Guidelines for Personal Information Security Specification], GB/T 35273-2020 (issued by Standardization Administration of China, 2020).
[284] *Xìnxī Ānquán Jìshù Jīqì Xuéxí Suànfǎ Ānquán Pínggū Guīfàn* (信息安全技术 机器学习算法安全评估规范) [Information Security Technology – Security Specification and Assessment Methods for Machine Learning Algorithms], GB/T 42888-2023 (issued by State Administration for Market Regulation & National Standardization Administration2024).
[285] *Xìnxī Ānquán Jìshù Gèrén Xìnxī Ānquán Yǐngxiǎng Pínggū Zhǐnán* (信息安全技术 个人信息安全影响评估指南) [Information Security Technology – Guidance for Personal Information Security Impact Assessment], GB/T 39335-2020 (issued by State Administration for Market Regulation & National Standardization Administration, 2021).
[286] *See supra note 248.*
[287] *See supra note 250.*
[288] *See* White & Case, *AI Watch: Global regulatory tracker – China* (2025), WHITE & CASE, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china .
[289] *See supra note 250.*

driving while safeguarding public interest. Still, usually these local regulations typically restate existing rules and rarely introduce new legal norms. They indeed must not contradict superior laws, which are under development[290].

Moreover, in the cases where high-level regulations are vague or do not fully address a matter, Normative Documents are enacted. They may cover a large range of topics, such as biometric identification, social credit, environmental protection, financial regulation and autonomous driving[291].

One of the first moves towards regulation on Artificial Intelligence was the 2017 launch by China's State Council of "Next Generation Artificial Intelligence Development Plan"[292], which highlights the country's objective to become a global leader in AI by 2030. It emphasizes Chinese government's goal to position AI as a driver of the country's technological and economic future[293]. During that formative stage, the government prioritized the formulation of policy mechanisms designed to catalyze technological innovation and accelerate industrial development[294].

Later then, since 2021, the country's regulatory approach to AI has evolved significantly. Several key regulations addressing the risks associated with AI technologies were introduced. The aim became to mitigate dangers such as deepfakes, disinformation and misinformation[295].

For instance, in December 2021 it was submitted the *Position Paper on regulating Military Applications of AI*[296], dealing with matters of primary importance such as the need for strategic security and military policy, ethics, technological safety, research and development, risk management

[290] *Id.*

[291] *Id.*

[292] State Council of the People's Republic of China, *New Generation Artificial Intelligence Development Plan*, State Council Document No.35 (2017).

[293] *See supra note 247.*

[294] *See supra note 250.*

[295] *See supra note 247.*

[296] *See* Ministry of Foreign Affairs, *Position Paper of the People's Republic of China on Regulating Military Applications of Artificial Intelligence (AI)* (2021), MINISTRY OF FOREIGN AFFAIRS THE PEOPLE'S REPUBLIC OF CHINA, https://www.mfa.gov.cn/eng/zy/wjzc/202405/t20240531_11367523.html .

and control, rule-making and international cooperation. All measures taken must be in the best interest of the country, thus avoiding conflicts and promoting stability[297].

Another the paper stressing the ethical importance of AI governance in China is the *Position Paper of the People's Republic of China on Strengthening Ethical Governance of Artificial Intelligence (AI)*[298] submitted in 2022. With it, China calls for the establishment of robust ethical norms, regulatory systems and accountability mechanisms to govern AI development. It emphasizes the protection of human rights, fairness and transparency in AI systems. Great importance is given also to R&D, to promote reliability, safety and eliminate biases and, to the promotion of international cooperations for technological progress[299].

Later then, in 2023, they were introduced the *Deep synthesis provisions*[300], with the aim to strengthen supervision over technologies like virtual reality and deep learning (the ones which create synthetic content such as video, audio or text). They apply to both service providers and users and, ensure that deepfake content is properly regulated and labelled[301].

In the same year, also the *Interim measures for Generative AI Services*[302] were enacted[303]. They have been released jointly by The Cyberspace Administration of China, the National Development and Reform Commission, the Ministry of Education, the Ministry of Science and Technology, the Ministry of Industry and Information Technology, the Ministry of Public Security and the National Radio and Television Administration[304]. With the scope to regulate publicly available Generative AI services, they require AI generated content to align with Core Socialist Values and with national

[297] *Id.*

[298] *See* Ministry of Foreign Affairs, *Position Paper of the People's Republic of China on Strengthening Ethical Governance of Artificial Intelligence (AI)* (2022), MINISTRY OF FOREIGN AFFAIRS THE PEOPLE'S REPUBLIC OF CHINA, ,https://www.fmprc.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/AI/202211/t20221117_10976730.html .

[299] *Id.*

[300] *Guójiā Yǔnxǔ Xìnxī Ānquán Jìshù Xìtǒng Jìshù Guīfàn* (国家允许信息安全技术系统技术规范) [National Permitted Information Security Technology System Technical Specifications], GB/T 35273-2020 (issued by Standardization Administration of China, 2020).

[301] *See supra note 247.*

[302] *Shēngchéng Shì Rén Gōng Zhìnéng Fúwù Guǎnlǐ Zànxíng Bànfǎ* (生成式人工智能服务管理暂行办法) [Interim Measures for the Administration of Generative Artificial Intelligence Services], issued by the Cyberspace Administration of China et al., 2023.

[303] See supra note 247.

[304] *See supra note 288.*

security and stability concepts. Following them, before releasing LLMs, companies must seek government approval, to ensure compliance with ethical and political standards[305]. If providers of generative AI services breach the AI Measures or other applicable laws, the relevant authorities may impose penalties under the *Cybersecurity Law*[306], the *Data Security Law*[307], the *PIPL*[308], the *Law on the Progress of Science and Technology*[309] and, any other relevant legal provisions[310]. In cases where existing laws or regulations do not provide clear guidance, authorities may issue warnings and require corrective actions within a specified timeframe. If providers fail to comply or if the violation is serious, service suspension may be enforced[311].

In 2023 and 2024, China's engagement in global AI safety efforts gained momentum through key events and contributions by prominent scientists and industry leaders. Ahead of the 2023 UK AI Safety Summit, Turing Awardee Andrew Yao and others participated in the Inaugural International Dialogues on AI Safety (IDAIS), producing a joint statement on mitigating frontier AI risks. The second IDAIS dialogue in Beijing further solidified collaboration with scientists and industry leaders endorsing redlines for AI development. Meanwhile, Shanghai AI Lab emerged as a leader in AI safety research and policy, releasing a report advocating for AI safety outputs as global public goods[312].

A further development of the *Interim Measures for Generative AI Services*[313] are the *Generative AI Content Labeling Requirements*[314], which have been approved and will be introduced in September 2025. They require all AI generated contents to be clearly labelled, trustworthy and transparent in their application[315]. They impose explicit and implicit labeling obligations on providers of online

[305] *See supra note 247.*

[306] *See supra note 276*

[307] *See supra note 275*

[308] *See supra note 274.*

[309] *Zhōnghuá Rénmín Gònghéguó Kēxué Jìshù Jìnbù Fǎ* (中华人民共和国科学技术进步法) [Law of the People's Republic of China on Progress of Science and Technology], 2022.

[310] *See supra note 288.*

[311] *Id.*

[312] *See supra note 250.*

[313] *See supra note 302.*

[314] *Rén Gōng Zhìnéng Shēngchéng Nèiróng Biāo Zhì Bànfǎ* (人工智能生成内容标识办法) [Measures for Labeling Artificial Intelligence-Generated Content], issued by the Cyberspace Administration of China et al., 2025.

[315] *See supra note 247.*

content distribution services and, on internet information service providers that create AI-generated content. They introduce two types of labels: the explicit ones, so visible indicators such as text and audios that inform users when content is AI-generated and, implicit labels, so data embedded within AI-generated content which contain details such as the service provider's name and content ID. Those rules require providers of online content distribution services to implement mechanisms to detect and reinforce AI content labeling, thus ensuring traceability. The AI contents are classified in three groups: confirmed (The implicit label is detected and the content is declared to be AI-generated), possible (No implicit label is detected, but the user reports the content as AI-generated) or suspected (Neither an implicit label is detected, nor the user report suggests an AI-generated content)[316].

Furthermore, a possible comprehensive framework for AI governance in China is the Chinese Academy of Social Sciences' *Model AI Law* (MAIL)[317], first introduced in 2021 and then revised in 2024. With it, the Chinese law adopts an approach to remain adaptable to technological advances, while maintaining core principles of safety, transparency, fairness and human oversight. It employs a risk management approach using a negative list system, where high-risk activities face stringent oversight while lower-risk innovations operate under simpler registry requirements. It establishes that AI stakeholders should delineate specific duties for developers, providers and users. Moreover, the Governance framework proposes a centralized approach to AI oversight. It recommends the establishment of a national AI authority to coordinate regulation, thereby avoiding fragmented regulatory landscapes[318]. The law addresses also legal liabilities. It focuses on accountability for stakeholders engaged in high-risk AI activities and includes provisions for exemptions where compliance measures are actively undertaken. Thus, fostering an environment where developers are encouraged to innovate without disproportionate fear of punitive actions. This measured approach

[316] *See* Yan Luo & Huezi Dan, *China Releases New Labeling Requirements for AI- Generated Content* (2025), COVINGTON, https://www.insideprivacy.com/international/china/china-releases-new-labeling-requirements-for-ai-generated-content/.

[317] *Rén Gōng Zhìnéng Fǎ Shìfàn Fǎ 1.0 Zhuānjiā Jiànyì Gǎo* (人工智能法 示范法 1.0 专家建议稿) [Artificial Intelligence Law, Model Law v. 1.0 (Expert Suggestion Draft)], issued by the Chinese Academy of Social Sciences, 2023.

[318] *See supra note 316.*

recognizes the uncertainties associated with AI and seeks to regulate it through an adaptive, principle-based framework, reflecting China's broader vision for managing emerging technologies[319].

Furthermore, in fall 2025, they will be started *Mandatory education initiatives*[320], with which students will be required to complete a least 8 hours of AI education per academic year. Those provisions are designed to promote AI literacy and foster innovation[321].

Moreover, there can be identified some regulations in the Chinese system, which overlap with AI-concerns. One of them are the *Regulations on the Administration of Network Data Security*[322] (Effective since January 2025), which cover aspects of AI such as data protection, cybersecurity, algorithmic discrimination and content safety. There are also the *Regulations on the Online Protection of Minors*[323] (Effective since January 2024), which address matters such as algorithmic addiction, by including the addiction from smart devices such as mobile phones[324].

The key for future legislation in China, as the AI Global regulatory tracker of White &Case suggests, is balancing technology innovation with risk control. The rise of domestic AI applications, such as DeepSeek, are speeding up the process of AI Law and, China might be able to come up soon with a Chinese model for AI governance[325].

3.4 Comparative analysis – Strengths, weaknesses and conflicts among these regulatory models

[319] *See supra note 250.*

[320] *See supra note 247.*

[321] *See supra note 247.*

[322] *Wǎngluò Shùjù Ānquán Guǎnlǐ Tiáolì* (网络数据安全管理条例) [Regulations on the Administration of Network Data Security], issued by the State Council of the People's Republic of China, 2025.

[323] *Wèichéngniánrén Wǎngluò Bǎohù Tiáolì* (未成年人网络保护条例) [Regulations on the Protection of Minors on the Internet], issued by the State Council of the People's Republic of China, Order No. 766, 2024.

[324] *See supra note 250.*

[325] *See supra note 288.*

AI regulations in different countries reflect each country's principles and ideologies. By looking at the differences among the regulations of the countries analyzed, some aspects may be highlighted.

China for instance, which adheres to Communist principles, aims at a society organized with collective ownership of resources and state-controlled production[326]. So, it tries to balance state-control and industry self- discipline[327].

European Union's approach to AI instead, being a collection of 27 countries following the principles of freedom, democracy, respect for human rights and supremacy of law, derived from the European Union Treaty[328], moves towards them. For this reason, EU's approach is risk-based and provides flexibility for the development and advancement of AI, by balancing innovation and ethical principles[329]. So, it provides comprehensive and stringent regulation[330].

Moreover, Unites States in which Liberalism, freedom and individual rights are the foundation principles, has an approach towards AI which aims at country's commitment to innovation, individual freedom and minimal government intervention[331]. Key points of a federate and flexible approach[332].

Russia instead, is far behind these other nations. It currently ranks 31st in the Global AI Index of 83 countries which have invested in AI, compared to for instance US and China which occupy respectively the first two places[333]. And, this is a result of the digital isolation that Russia experienced after 2022, due to the Russian war on Ukraine[334]. For these reasons, it consequently aims at strategic alignment with national goals[335].

[326] *See* Faisal Santiago et al., *A Comparative Analysis of Artificial Intelligence Regulatory Law in Asia, Europe, and America* (2024), SHS WEB OF CONFERENCES, https://www.shs-conferences.org/articles/shsconf/abs/2024/24/shsconf_diges-grace2024_07006/shsconf_diges-grace2024_07006.html .

[327] *See* Maulen Alimkanov, *Comparative Analysis of International AI Regulatory Approaches: The United States, European Union, Canada, China, Kazakhstan, Russia* (2024), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4873053 .

[328] Consolidated Version of the Treaty on European Union 2012 O.J. (C 326/13) 1.

[329] *See supra note 326.*

[330] *See supra note 327.*

[331] *See supra note 326.*

[332] *See supra note 327.*

[333] *See* Tortoise – Global Ai, *The Global AI Index*, TORTOISE MEDIA, https://www.tortoisemedia.com/data/global-ai

[334] *See* Justin Sherman, *Russia's digital tech isolationism: Domestic innovation, digital fragmentation, and the Kremlin's push to replace Western digital technology* (2024), ATLANTIC COUNCIL, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-digital-tech-isolationism/ .

[335] *See supra note 327.*

Going more deeply, the 2024 EU *AI Act*[336] is considered the first comprehensive AI law. It represents joint efforts from various EU bodies, such as the European Commission, the European Parliament and the European council. It was influenced by some European National Governments, like the France's premier Macron's lobbying per exemptions for open-source AI providers such as Mistral, the German pro open-source non-profit LAION and the lobbying of some Big Tech groups. Besides regulating the EU single market, this Act is regarded as the effort by the European Commission to establish themselves as the leading AI rule makers globally[337].

After the adoption of the *GDPR*[338] in 2016, it could be noticed the so called "Brussels Effect", so the fact that companies across the world began to prioritize compliance with European law out of economic necessity. There was also the "de jure" effect, so that countries with a lack of regulatory capacity incorporated EU laws instead. For instance, the Philippines incorporated the right to be forgotten into their *Data Privacy Act*[339] of 2012. Indeed, it is believed that The EU *Act*[340] may become the de-facto standard for AI governance in the Western developing world[341].

It may be noted that in terms of comprehensive legal frameworks, there is one State that in US that has stood out: California. It distinguished itself for the broad and effective regulations enacted. The main one is the *California Senate Bill 1047*[342], introduced in February 2024. It aims to establish a comprehensive AI regulatory framework in California focused on frontier models. There are ongoing debates about the influence of this Bill over US competitiveness. As John Chun, expert of Cornell University, in his article: "Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US"[343] highlights, this Bill, unlike the EU *AI Act*[344], which adopts a comprehensive

[336] See supra note 69.

[337] *See* Jon Chun et al., *Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US* (2024), ARXIV – CORNELL UNIVERSITY, https://arxiv.org/abs/2410.21279 .

[338] *See supra note 71.*

[339] *Republic Act No. 10173*, An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes, § 1, 2012.

[340] *See supra note 69.*

[341] *See supra note 337.*

[342] S.B. 2047, 2023-2024 Leg., Reg. Sess.(Cal. 2024).

[343] *See supra note 337.*

[344] *See supra note 69.*

risk-based approach to AI regulation, focuses more narrowly on high-impact AI systems, particularly those trained using substantial computational resources. This approach reflects a philosophy that prioritizes regulating the most powerful and influential AI models that have the greatest societal impacts. However, it is unclear whether the Californian Bill adopts a similar approach to the European Union Act[345], which in turn provides a degree of flexibility in implementation and allows for personalized requirements for specific high-risk applications[346].

So, while the European Union's *AI Act*[347] and *GDPR*[348] emphasize stringent data protection and transparency, striking a balance between innovation and ethical considerations, in US, Initiatives like the *Blueprint for an AI Bill of Rights*[349] and the *AI Risk Management Framework*[350] aim to foster ethical AI usage while promoting a free-market, innovation-driven environment. This reflects US' attitude towards liberalism and freedom[351], which is further enforced by the current Trump's deregulatory approach[352]. So, it aims at reaching principles which would guide global AI regulation, ensuring responsible development while maximizing benefits and minimizing risks[353].

China's government is often described as autocratic and socialist instead, as an article of Francisca Romana Nanik Alfiani and Faisal Santiago about the comparative analysis of regulation in various countries suggests: its legal framework reflects the principles of *fahzi* or *yifazhiguo*, which translate into "Government based on law" [354]. The Chinese legal system is a Socialist system following the civil law model, influenced by German Civil Law and Chinese legal practices. In China, AI

[345] *See supra note 69.*
[346] *See supra note 337.*
[347] *See supra note 69.*
[348] *See supra note 71.*
[349] *See supra note 172.*
[350] See Elham Tabassi, *Artificial Intelligence Risk Management Framework* (2023), NIST, https://doi.org/10.6028/NIST.AI.100-1.
[351] *See supra note 326.*
[352] *See* Mattew Kirk et al., *Key Insights on President Trump's New AI Executive Order and Policy % Regulatory Implications* (2025), SQUIRE PATTON BOGGS, https://www.squirepattonboggs.com/en/insights/publications/2025/02/key-insights-on-president-trumps-new-ai-executive-order-and-policy-regulatory-implications.
[353] *See supra note 326.*
[354] *Id.*

regulations, especially in surveillance, help maintain State Control but, raise ethical concerns about privacy and human rights[355].

China's approach to AI governance, as John Chun suggests, is a "hybrid between the centralized, top-down approach of the EU and the decentralized, free-market of competing interests in the US"[356]. Indeed, like the European Union, China emphasizes safety, individual protections, and social harmony through guidance and enforcement. And, like the US, it prioritizes innovation and economic development with a mix of decentralized provincial control. This hybrid approach earns benefits from both EU and US models: China seeks to benefit from the coherence of the EU *AI Act*[357] and from the practical US approach[358].

However, unlike the risk-based approach of the EU, China had preferred the sector-specific US approach for laws tailored to specific use-cases, like in data privacy, recommendation algorithms or generative AI field. The Chinese AI regulations are the product of a long process involving stakeholders such as bureaucrats, academics and corporations. The Central Government relies on these experts to obtain outcomes aligned with Chinese and socialist ideology. On paper, China has perhaps the most onerous AI requirements compared to EU and US, including *model registration laws*[359], *rules for data management*[360], and *provisions for monitoring compliance*[361][362].

As a result, it emerges that the United States emphasize innovation, with fewer regulatory constraints compared to Europe, China and Russia[363].

[355] *Id.*
[356] *See supra note 337.*
[357] *See supra note 69.*
[358] *See supra note 337.*
[359] Interim Measures for the Management of Generative AI Services, issued by the Cyberspace Administration of China et al., 2023.
[360] *Measures for the Management of Scientific Data* (科学数据管理办法), issued by the State Council of the People's Republic of China, 2018.
[361] *See supra note 359.*
[362] *See supra note 337.*
[363] *See supra note 326.*

However, despite such rigorous guidelines, the regulation enforcement in China is relatively lax. Small companies fly under the radar as long as they do not have a large public presence. And, all this approach allows economic growth, innovation and international competitiveness[364].

Conversely, the strict law enforcement comes into play when destabilizing patterns arise. At that point, market disruptions can be caused and lead to strictly punitive measures. An example may be the penalties inflicted in 2020-2022 to powerful tech and financial corporations, such as Alibaba and Ant Group which could challenge the government authority[365].

Enforcement in EU and US instead, is someway different. The *EU AI Act*[366] is premised upon prevention: general guidelines and penalties prohibit activities unless explicitly permitted. In contrast, the US model is a lot permissive: it promotes innovation through competition, encourages decentralized self-regulation, and relies upon existing laws and regulations against abusive, illegal and negligent practices[367]. While China adopts a vertical approach that uses laws to tackle specific issues with focused legislation, the EU takes a horizontal approach that aims to regulate AI comprehensively across different sectors[368].

China's Social Credit System uses advanced technologies, like AI for facial recognition and monitors, to assess citizens' behavior, assigning scores based on factors such as financial history and social interactions. However, this is an extremely polarized approach compared to other governing bodies. EU reviews regulations to give citizens explicit use rights over facial recognition data, and the US law instead, has multiple definitions of privacy. Josh China and Liza Lin, authors of "Surveillance State"[369] argue that China has redefined privacy in a new social contract that places onus on companies and sells citizens data in exchange for precise governance that increases security and convenience[370].

[364] *See supra note 337.*
[365] *Id.*
[366] *See supra note 69.*
[367] *See supra note 337.*
[368] *See* Yannic Mahé, *Divergent Paths: Comparing AI Regulation in the US, EU, and China* (2024), LINKEDIN, https://www.linkedin.com/pulse/divergent-paths-comparing-ai-regulation-us-eu-china-yannick-mahé-ztlre/ .
[369] *See* JOSH CHINA AND LIZA LIN, SURVEILLANCE STATE, (1st ed. 2022)
[370] *See supra note 242.*

Moreover, even though EU is lagging behind US' and China's innovation, it has taken proactive measures to address the risks associated with AI deployment. Just as *GDPR*[371] has changed privacy practices worldwide, the EU *AI Act*[372] has posed EU as a regulatory trailblazer in the digital age, thus letting it have a relevant impact globally[373].

China emphasizes control over AI development to safeguard against losing control, while the EU focuses on protecting personal data privacy and the US aim to guard against fraud, unintended bias, discrimination and infringements on privacy[374].

Extreme differences in regulations may lead companies to exit a certain jurisdiction altogether. Meta and Google for instance, left jurisdictions such as China, Russia, Spain, Australia and Canada rather than comply with local regulatory requirements. And of course, the opposite dynamic can also happen. Large companies may adopt strict standards or lobby countries to harmonize their regulatory regimes through international agreements. The outcome will depend on whether the gains from the imposition of the national law overcome the losses due to regulatory fragmentation. Meta is also being forced to change part of its business model in Europe, adopting a subscription model in response to local privacy regulatory requirements[375] .

European companies have used this international competition to shape the drafting of the EU's *AI Act*[376] to make it more EU-company-friendly. Moreover, a coalition of companies uses this international competition to push for the reforms of other EU regulations that they dislike, such as *Data Privacy Laws*[377]. In the US instead, tech companies have used the innovation race to

[371] *See supra note 71.*
[372] *See supra note 69.*
[373] *See supra note 368.*
[374] *See supra note 368.*
[375] *See* Filippo Lancieri et al., *AI Regulation: Competition, Arbitrage & Regulatory Capture* (2025), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5049259 .
[376] *See supra note 69.*
[377] *Regulation (EU) 2016/679*, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

successfully pressure the California Governor to veto a 2024 bill[378] that would have imposed restrictions and safeguards on the development of AI models in the State[379].

Governments use a combination of regulatory regimes and subsidies to ensure control over the different layers of the AI supply chain. Companies instead, try to put Governments against one another to gain additional leverage in international negotiations and, to weaken restrictions that they see as detrimental to their business models[380].

Moreover, another pattern which distinguishes the US from its EU comparators, is the weakness of its social partnerships and of its union management relations for institutional environment. Unlike Germany and Northern Countries, where multiple level of workers are integrated into labor relations by law, the US offers a singular, firm-based, adversarial framework, thus allowing to little power for workers voice and over AI[381].

Some differences emerge even from the extra-territorial applications of laws in the various countries. Indeed, while the EU *AI Act*[382] and China's regulatory frameworks declare themselves to apply extraterritorially, by covering any provider or deployer of AI systems used in EU, the US and Russia have not established a comprehensive federal AI regulation with extraterritorial scope[383].

The impact on innovation and ethics also varies. While EU's regulations ensure ethical standards and public trust but by risking to slow innovation, the US approach promotes rapid innovation by risking ethical inconsistencies. China's approach instead, aims for both innovation and ethics, but faces control-related challenges and, Russia focuses more on strategic alignment, buy by risking to hinder broader ethical AI advancements[384].

[378] *See supra note 375.*
[379] *See supra note 375.*
[380] *Id.*
[381] *See* Adam Set Litwin et al., *A Forum on Workplace AI Regulation Around the World*, 77 ILR Rev. 14 (2024).
[382] *See supra note 69.*
[383] *See supra note 327.*
[384] *Id.*

Indeed, although the EU *AI Act*[385] is being accused of impeding innovation, the lack of explicit ethical safeguards and risk mitigation measures in the *Trump Executive Order*[386] could weaken the ability of US companies to compete in European markets. Those companies operating across various jurisdictions will have to adopt flexible compliance strategies to account for varying regulatory standards. Trump's deregulation strategy is risking to give the perception that the US prioritizes short-term innovation gains over long-term ethical considerations, by potentially alienating allies and partners. Squire Patton Boogs' Professionals pose the question on whether Trump's approach will preserve and enhance US leadership in AI or in turn, will allow China to build a more powerful AI platform. The US approach will attract investments and innovations to US AI companies, but China may be able to arrive at a collaborative engagement with international AI governance initiatives, in order to position itself as an international leader in AI[387].

Moreover, professor's Anu Bradford work: "Digital Empires: The Global Battle to Regulate Technology"[388], has detailed the geopolitical competition between US, EU and China to impose their different visions of digital regulation. This competition materializes itself in measures such as US working with EU to restrict China's access to high-end GPUs and other advanced AI chips[389].

In conclusion, AI regulatory models in China, EU, US and Russia often differ basing on the country's principles: while EU adopts a comprehensive and preventive approach, China, US and Russia follow more reactive and fragmented strategies. Still, all frameworks share core principles such as ethics, data privacy, algorithmic transparency, bias mitigation, explainability and international cooperation. China's state-controlled approach focuses on balancing social stability with individual freedoms. While regulations like the *AI act*[390] and Data Protection Laws, aim at maximizing AI's benefits while addressing ethical concerns and maintaining strict oversight[391].

[385] See supra note 69.

[386] See supra note 196.

[387] *See supra note 352.*

[388] ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY (1st ed. 2023).

[389] *See supra note 375.*

[390] *See supra note 69.*

[391] *See supra note 234.*

3.5 The reaching of international agreements for the creation and usage of AI

During 2017-2018 AI first reports and policies were created and, education, training and funds were provided. Yet, after a few years, still BRICS nations did not have any special regulations for AI. In 2020-2021 the first regulations started to be approved and were mainly focused on *OECD principles*[392]. OECD had indeed developed 5 basic universal principles for responsible stewardship of AI trustworthy. First of all, AI should be advantageous to humans and environment through sustainable development, inclusive growth and well-being. Then, AI systems must be established to follow human rights, diversity, rule of law and democratic values and, must assure fair society intervention wherever needed. Moreover, responsible and transparent disclosure around AI systems should be enhanced, in order to let people understand and eventually challenge AI based results. Indeed AI systems may perform in secure, safe and robust way and stronger risks must be managed continually. Lastly, individuals and sectors that establish, develop and deploy AI systems must be held accountable for their appropriate functioning in line with mentioned principles[393].

However, for the first time, the first ever binding international Treaty on Artificial Intelligence was recently adopted[394]. On 18th May 2024, after 2 years of negotiations, the Committee on Artificial Intelligence (CAI) (Established in 2022 by the Council of Europe)[395] has enacted the *Council of Europe Framework convention on Artificial Intelligence and Human Rights, Democracy, and the*

[392] *See Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2024), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[393] *See* Nibedita Basu et al., *COMPARATIVE ANALYSIS OF LAWS IN AI*, 5 SDG Rev. 17,18 (2024).

[394] *See* José-Miguel Bello, *A first step on the long road to global AI regulation* (2024), THE INTERPRETER, https://www.lowyinstitute.org/the-interpreter/first-step-long-road-global-ai-regulation .

[395] *See* Future of Privacy Forum, *THE WORLD'S FIRST BINDING TREATY ON ARTIFICIAL INTELLIGENCE, HUMAN RIGHTS, DEMOCRACY, AND THE RULE OF LAW: REGULATION OF AI IN BROAD STROKES* (2024), FUTURE OF PRIVACY FORUM, https://fpf.org/blog/the-worlds-first-binding-treaty-on-artificial-intelligence-human-rights-democracy-and-the-rule-of-law-regulation-of-ai-in-broad-strokes/ .

Rule of Law (CEST No.225)[396] ("Framework Convention"/"Convention"). It is one of the first times that US and EU have formally aligned their views on AI regulation[397].

The *Framework Convention* was drafted by the 46 member States of the Council of Europe (COE), together with the participation of other observer states[398] (which cooperate with COE, participate to Committees and become parties to its conventions[399]). As of today, its signatories are: Andorra, Georgia, Iceland, Liechtenstein, Montenegro, Norway, Republic of Moldova, San Marino, Switzerland, UK, Canada, EU, Japan, Israel and US[400]. This Treaty is open to all countries, and while not a signatory, Australia participated in the negotiations[401].

However, the *Framework Convention* has made it evident the fact that there is a real division between Western democracies and other jurisdictions such as Asia, Saudi Arabia, Pakistan and Venezuela, which are indeed notably absent. In these last countries, the current deployments of AI seem to go against the fundamental principles of human dignity and protection of individuals, which are conversely at the center of the Western culture[402].

The *Framework Convention* aims at establishing a risk-based approach to regulate AI and common principles related to activities withing the entire lifecycle of AI systems, with the constant respect of human rights[403].

Its general principles include:

- Respect for human dignity and individual autonomy (Art.7)
- Transparency and oversight (Art.8)
- Safe innovation: establishment of controlled environments for developing and testing systems (Art. 13)

[396] *See* Council of Europe, *The Framework Convention on Artificial Intelligence,* COUNCIL OF EUROPE PORTAL, https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence .

[397] *See supra note 394.*

[398] *Id.*

[399] *See supra note 395.*

[400] *See supra note 396.*

[401] *See supra note 394.*

[402] *Id.*

[403] *Id.*

- Accountability and responsibility for adverse impacts on human rights, democracy and rule of law (Art. 9)
- Reliability, trust, quality and security (Art. 12)
- Equality and non-discrimination (Art. 10)
- Respect for privacy of individuals and personal data protection (Art. 11) [404]

States Parties to the *Framework convention*, have to adopt appropriate legislative measures to give effect to the provisions of this instrument in their domestic laws[405]. It complements existing international standards of human rights, democracy and the rule of law and, aims to fill gaps resulting from rapid technological advances. Moreover, important to notice is the fact that it does not regulate technology and it is essentially technology-neutral[406].

The *Framework convention* has the potential to affect ongoing national and regional efforts to design and adopt binding AI laws and, may be uniquely positioned to advance interoperability[407].

The work was initiated in 2019, when the ad hoc Committee on Artificial Intelligence (CAHAI) was tasked to examine the feasibility of such an instrument. Then, in 2022, the Committee on Artificial Intelligence (CAI) started to draft and negotiate the text[408].

One of the first challenges that emerged from International Cooperation was the need to agree on a common definition. The matter is addressed in Article 2, with the adoption of the OECD's definition of an AI system. It is indeed classified as a "Machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment"[409].

[404] *See supra note 396.*
[405] *See supra note 395.*
[406] *See supra note 396.*
[407] *See supra note 395.*
[408] *See supra note 396*
[409] *Id.*

Article 3 instead, declares the *Framework* to address: "the activities within the lifecycle of artificial intelligence systems that have the potential to interfere with human rights, democracy and the rule of law"[410]. Following the *Framework*, each Party has to apply the principles undertaken by public authorities or private actors on their behalf within the lifecycle of AI systems. Private entities must satisfy two conditions. First, the country where they operate, develop, or deploy their AI system must be a State Party to the Convention. Second, private actors should design, deploy or develop AI products on behalf of State Parties' public authorities. However, Article 3(2) provides an exception: for AI systems protecting national security interest, the Parties are not required to apply the obligations of the *Framework*. Still, State Parties shall comply to international laws and human rights obligations. Similarly, the *Framework Convention* will not apply to R&D activities regarding AI systems that are not yet available for use, unless their testing has the potential to interfere with human rights, or to matters relating to national defense[411].

Article 4 and 5 of the *Framework Convention* on AI instead, address the consistency of the activities within the lifecycle of the AI systems, with obligations to protect human rights. This includes seeking to protect individuals' fair access and participation in public debate and their ability to freely form opinions. Articles 7 to 13, provide the aforementioned fundamental principles on which the *Framework* lays its foundations. Further articles then concern the obligations of State Parties to guarantee human rights in the deployment of AI and the possibility for States to grant wider protection in their domestic laws[412].

There can be highlighted similarities with the EU *AI Act*[413] in the formulation of the *Framework*'s risk-based approach. They are traceable by particularly looking at the requirements for risk monitoring, documentation and testing. However, it does not take a layered approach to risk, from

[410] *Id.*

[411] *See supra note 395.*

[412] *Id.*

[413] *See supra note 69.*

limited to high risk, so it does not prescribe contexts and use cases in which AI systems may be prohibited[414].

Furthermore, The *Preamble of the Framework Convention*[415] stresses the importance of cooperation among States and of trying to extend it even more [416].

Usually, International Cooperation and Coordination of AI is a matter of concern of the OECD AI principles and, at the intergovernmental level, also of the Group of 7 (G7), which approved an *International set of Guiding Principles on AI*[417] and a voluntary *Code of Conduct for AI developers*[418] [419]. The *Framework Convention* on AI instead, aims at establishing its own proposal for furthering International Cooperation on the basis of a two-pronged approach. At first, in Art. 23 it calls for the formation of a Conference of the Parties, and, in Art.25 it states that Parties have to exchange relevant information among themselves and, assist States that are not Parties to the Convention to act consistently with its requirements, with a view to becoming Parties to it[420].

Moreover, the *Framework Convention* requires States to document the relevant information of their AI systems and of their usage. Information must be sufficient to allow people to challenge the decisions made through the use of the system or based substantially on it, or to challenge the system itself. This way the *Framework* is able to safeguard and guarantee procedural rights to States. Also, there has to be the effective possibility to lodge a complaint to competent authorities. States must provide effective procedural guarantees, safeguards and rights to affected people whose enjoyment of human rights and fundamental freedoms were impaired. States ultimately must notice users that they are interacting with AI and not with a human being[421] .

[414] *See supra note 395.*

[415] See supra note 396.

[416] *See supra note 395.*

[417] See Shaping Europe's digital future, *Commission welcomes G7 leaders' agreement on Guiding Principles and a Code of Conduct on Artificial Intelligence* (2023), DIGITAL STRATEGY, https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-g7-leaders-agreement-guiding-principles-and-code-conduct-artificial

[418] *Id.*

[419] *See supra note 395.*

[420] *See supra note 395.*

[421] *See supra note 396..*

Furthermore, concerning the risks and impact management requirements for the States: they must carry out risk and impact assessments in respect of actual and potential impacts on human rights, democracy and the rule of law. They must also establish sufficient prevention and mitigation measures as a result of the implementation of these assessments. And also, authorities have the possibility to introduce ban or moratoria on certain applications of AI systems ("red lines")[422].

In order to monitor the application of the *Framework*, a follow-up mechanism is established: The Conference of the Parties. It is made up of official representatives of the Parties of the Convention, who will determine the extent to which its provisions are being implemented. The findings extracted and the recommendations filed will help States to ensure compliance with the *Framework* and will guarantee its long-term effectiveness. Moreover, this follow-up mechanism shall facilitate the cooperation with the important stakeholders through public hearings about relevant aspects of the implementation of the *Framework Convention*[423].

So, the underlying concept of the *Framework Convention on AI* is to act as a foundational umbrella, which provides foundational principles, but beyond which, more specific rules can be adopted at country level. It has a strong foundation in human rights law, respect for equality and non-discrimination and, human dignity and privacy[424].

4. Liability for AI systems

The potential of Artificial Intelligence has grown exponentially in last years. However, apart from generating value, it has also the possibility to create huge risks. For now and for the foreseeable future, AI systems' operations will not yet be fully autonomous, so, in order to reduce AI-related harm, it is important to provide appropriate incentives to the human parties involved[425].

[422] *Id.*

[423] *See supra note 396.*

[424] *See supra note 395.*

[425] *See* Shu Li et al., *Liability Rules for AI-Related Harm: Law and Economics Lessons for a European Approach*, 2022 CUP 1.

AI for instance has the potential to create vulnerabilities such as cyberattacks, errors in data processing, bias and production of fake information. Failing to take appropriate precautions against these attacks can lead to a breach of fiduciary duties of directors and officers and, to the consequent attribution of liability, thus damaging the reputation of a company and causing it financial loss[426].

Indeed, since these political issues have the potential to generate corporate risk, good corporate governance practices can help hindering them,thereby minimizing the potential for financial impacts on the corporation[427].

The usability of AI represents a dilemma for businesses and corporate fiduciaries. Too little reliance on AI may impair a company by positioning it too far behind its competitors, thus inferring a breach of the standards of care. But at the same, an excessive reliance on AI can still damage a company's operations and reputation, due to the risks deriving from legal challenges. So, it is always important to understand the dangers of using AI and to take measures to mitigate them[428].

Indeed, it is vital for boards to comply with their fiduciary *duties of oversight* and *risk mitigation*. All AI-facilitated processes must be supervised, and frequent controls on data security and AI vulnerabilities must be performed. For these purposes, companies can select AI structures that best fit their business needs, even a well-defined insurance can help [429].

The problem is that AI developers keep the algorithms of their technologies under lock, so, this lack of transparency makes it hard to determine the cause of errors. Thus, here comes the necessity for clear and effective laws to be made in practice[430].

[426] *See* Richik Sarkar et al., *Mitigating Board and Corporate Fiduciary Risks of AI*, 2025 Risk Management Magazine 1.

[427] *See* Kai Zenner, *An AI Liability Regulation would complete the EU's AI strategy* (2025), CEPS, https://www.ceps.eu/an-ai-liability-regulation-would-complete-the-eus-ai-strategy/ .

[428] *See supra note 426.*

[429] *Id.*

[430] *Id.*

In conclusion, the liability discussion will mainly concern Generative AI, since the risks posed to directors and officers are mainly derived from the generation of content by AI systems acting on their own capabilities[431].

4.1 AI and Fiduciary duties (*Caremark* standard) – Exploring directors' liability for failing to oversee AI risks

Generative AI is rapidly reshaping our daily lives, changing how we communicate, acquire knowledge and make both personal and professional choices. Nowhere is the risk, more than in an organization accountable to a myriad of stakeholders: the US publicly held companies[432].

Those companies can be both consumers and developers of GenAI systems. Common ways in which GenAI is used include: data analysis and insights, customer services and support, financial analysis and fraud detection, automation and quality control in production and operation management and, marketing and sales[433].

When implementing GenAI systems, the board and the management team must always justify the corporation's use of AI, so that it aligns with corporation's business operations, financial goals and shareholder interests. Indeed, publicly held companies that develop and sell GenAI systems have different obligations than those companies which only use them in their operations. When implementing AI products, publicly held companies must take into consideration the duty of supervision and the compliance measures that need to be taken[434].

Corporate governance principles require directors and officers to manage corporations consistently with their fiduciary duty to act in the best interest of shareholders. The board's specific fiduciary duty indeed, comprises two specific obligations: the *Duty of Care* (Addressed by the case *Smith v. Van*

[431] *See* Joseph R. Tiano Jr. et al., *The Duty of Supervision in the Age of Generative AI: Urgent Mandates for a Public Company's Board of Directors and Its Executive and Legal Team*, 2024 Bus. Law Today 1.

[432] *Id.*

[433] See supra note 431.

[434] *Id.*

Gorkom[435]) and the *Duty of Loyalty* (Addressed by the case *Cede & Co. v. Technicolor, Inc.*[436]). This last obligation, as will be better analyzed in the following part, provides an important liability which has been addressed by the *In re Caremark International Inc. Derivative Litigation*[437], the Duty of Oversight. The oversight liability of directors, as established by *Caremark* is a: "duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists"[438]. Thus, at the beginning, this kind of liability was subsumed in the *Duty of Care*, but as the case *Stone v. Ritter*[439] has further clarified, it falls within the *Duty of Loyalty* of the board, since it stems from a duty to act in good faith[440].

The first of the aforementioned duties, the *Duty of Care*, provides that corporate directors are obliged to make well-informed decisions in the best interest of the company. The second one instead, the *Duty of Loyalty*, requires directors to act in good faith and prioritize the company's interests over personal gain, thus supervising proactively the conduct of corporate subordinates[441].

In this section, it will be analyzed deeply the oversight liability (duty of oversight, or of supervision) of the board, derived from *In re Caremark International Inc. Derivative Litigation* of 1996[442].

In that case, the shareholders of the company Caremark International, alleged that they were injured by Caremark employees' violation of Federal and State laws applicable to healthcare providers, thus resulting in a federal mail fraud charge against the company. Consequently, Caremark agreed to reimburse various parties approximately $250 million. Still, the shareholders decided to file a

[435] Smith v. Van Gorkom, 488 A.2d 858 (Del. 1985).
[436] Cede & Co. v. Technicolor, Inc., 634 A.2d 345 (Del. 1994).
[437] In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).
[438] *Id.*
[439] *Stone v. Ritter*, 911 A.2d 362 (Del. 2006).
[440] *See* Gregory A. Markel et al., *A Director's Duty of Oversight after Marchand in "Caremark" Case* (2022), HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE, https://corpgov.law.harvard.edu/2022/01/23/a-directors-duty-of-oversight-after-marchand-in-caremark-case/ .
[441] *See* Lexi Legal Law, *The Legal Future: Artificial Intelligence and Corporate Law* (2025), MONDAQ, https://www.mondaq.com/turkey/corporate-governance/1566104/the-legal-future-artificial-intelligence-and-corporate-law.
[442] *See supra note 437.*

derivative action against the company's directors, alleging that they had breached their fiduciary *Duty of Care* by failing to actively monitor corporate governance[443].

After numerous speculations and evaluations, the Delaware Court of Chancery came up with the new *Caremark* Standard of oversight to be imposed in these cases, which at the time was subsumed into the *Duty of Care*. So that the board has: a "duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards"[444]. The Caremark court later clarified that a "lack of good faith" derives from "a sustained or systematic failure of the board to exercise oversight- such as an utter failure to attempt to assure a reasonable information and reporting system exist"[445].

One of the first cases in which the Delaware Supreme Court used the Caremark Standard of Oversight was in *Stone v. Ritter*[446]. In that occasion, the Court had the possibility to implement it, by stating that director's oversight liability is conditioned upon: "(a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, [the directors] consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention"[447]. Thus, failing to prove clear under the *Duty of Loyalty* depends on the of lack of good faith[448].

From now on, the *Caremark* Duty of Oversight will always be protected under the *Duty of Loyalty* instead of the *Duty of Care*[449].

As of today, the Duty of Supervision is composed of two prongs. The first requirement tasks the board of directors with ensuring that the company's reporting system is effective and that critical information reaches them promptly. Moreover, if the board meets the standard in the first prong, it

[443] *See* Amy Antoniolli et al., *ESG Update: Corporate Directors May Be Obligated to Assess Political Risk*, 2025 Nat. L. Rev. 1.
[444] See supra note 437.
[445] *Id.*
[446] *See supra note 439*
[447] Id.
[448] *See supra note 431.*
[449] *Id.*

can still violate the Duty of Supervision with the second prong, if it shows a lack of good faith caused by a director's systematic failure to exercise reasonable oversight[450].

However, the lack of good faith is a very difficult pattern to prove, and in these terms, the case *Marchand v. Barnhill*[451] of 2019 helped. The Court in that case has lowered the pleading requirement for oversight claims. It reiterated that the board has a duty to exercise oversight and to monitor the "corporation's operational viability, legal compliance and financial performance"[452]. The board has to make a good faith attempt, following the *Duty of Loyalty*, to implement reasonable systems of information and to monitor the existing systems, thus preventing the emergence of a "mission-critical risk", so a unique and extraordinary risk, for the company[453].

The characteristics of this standard were further clarified in a derivative suit against Boeing corporation. In *In re Boeing Company Derivative Litigation*[454] the Court permitted a Caremark claim to proceed against Boeing's board of directors, since a director had acknowledged the board's scarce oversight of safety measures. So, because of the fact that scarce safety is indeed a mission-critical risk for an aircraft company, an enhanced scrutiny of board's oversight would have been justified[455].

The definition of "mission-critical" was further clarified in cases like *Teamsters Local 443 Health Servs. & Ins. Plan v. Chou*[456], *In re Clovis Oncology, Inc. Derivative Litigation*[457] and *Constr. Indus. Laborers Pension Fund v. Bingle*[458]. The definition provides that instances that a Court may consider *mission-critical* are risks arising from compliance with positive law, which pertain to key operations of a company operating in multiple segments, where a failure to comply could impair the company's ability to do business. It refers also to the risks arising from those operations directly in contrast with the central purpose of the company's business and which impair the company's ability to do business.

[450] *Id.*
[451] Marchand v. Barnhill, 212 A.3d 805 (Del. 2019).
[452] *Id.*
[453] *See supra note 440..*
[454] In re The Boeing Co. Derivative Litig., C.A. No. 2019-0907-MTZ, 2021 WL 4059934 (Del. Ch. 2021).
[455] *See supra note 431.*
[456] Teamsters Local 443 Health Servs. & Ins. Plan v. Chou, C.A. No. 2019-0816-SG, 2020 WL 5028065 (Del. Ch. 2020).
[457] In re Clovis Oncology, Inc. Derivative Litig., C.A. No. 2017-0222-JRS, 2019 WL 5054136 (Del. Ch. Oct. 1, 2019).
[458] Constr. Indus. Laborers Pension Fund v. Bingle, C.A. No. 2021-0940-SG, 2022 WL 4102492 (Del. Ch. 2022).

Moreover, it concerns risks that do not derive from compliance with positive law, but which are about the business components on which a company strongly relies on. They should be so critical for which non-binding soft law exists and for which there are industry regulations and rules which indicate a duty to act on such risks[459].

Other further developments of the *Caremark* Standard include the extension of the Duty of Supervision beyond the board, to executive management officers. It was put in practice in the case *In re McDonald's Corporation Stockholder Derivative Litigation*[460] in 2023. Where executive officers, since being agents reporting to the board, were deemed to have the obligation to "identify red flags, report upward, and address the [red flags] if they fall within the officer's area of responsibility"[461][462]. Furthermore, in *Clem v. Skinner*[463], in 2024, the court held that *Caremark* claims should be limited to circumstances where there has been a corporate calamity and the injury is not just financial[464].

So, in short, key points of *Caremark* liability standard under Delaware law include first of all the Duty of Oversight, so a duty for directors to make a good faith effort to oversee companies' operations and their compliance with law. Then, there is the obligation for directors to implement and monitor systems that provide accurate and timely information about the corporation's compliance with legal obligations. Moreover, in order to establish a breach of *Caremark* duty, plaintiffs must show either that directors have utterly failed to implement any reporting or information system and control, or, that they have implemented it, but by consciously failing to monitor and oversee its operations. Then, there is the fact that directors are generally protected if a good faith effort to fulfill their oversight responsibility was done. And lastly, it remains an high threshold for liability, so in order to prove a

[459] *See* Edmond & Lily Safra, *Post #6: The Caremark Rule and Board Level AI Risk Management* (2024), CENTER FOR ETHICS – HARVARD UNIVERSITY, https://www.ethics.harvard.edu/blog/post-6-caremark-rule-and-board-level-ai-risk-management%C2%A0 .
[460] In re McDonald's Corp. Stockholder Derivative Litig., C.A. No. 2021-0324-JTL, 291 A.3d 652 (Del. Ch. 2023).
[461] *Id.*
[462] *See supra note 431.*
[463] *Clem v. Skinner*, C.A. No. 2021-0240-LWW, 2024 WL 1050900 (Del. Ch. 2024).
[464] *See* Gail Weinstein et al., *2024 Caremark Developments: Has the Court's Approach Schifted?* (2024), HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE, https://corpgov.law.harvard.edu/2024/05/20/2024-caremark-developments-has-the-courts-approach-shifted/ .

breach of a *Caremark* duty, bad faith or conscious disregard by directors of their duties has to be proved[465].

For these reasons, *Caremark* remains one of the most difficult standards to plead. The demonstration of bad faith is complex,but can still be viable[466].

There are several possible contexts where AI risks may yield to *Caremark* claims. They include but are not limited to: where AI is the very essence of the company's business, where AI is a central component of the company's core operations, where AI is part of or supports the company's operations but in a high-risk era and, when there is a routine AI use that results in foreseeable harm[467].

In this matter, there is an article of Tiano, from the Business Law Review called: "The Duty of Supervision in the Age of Generative AI: Urgent Mandates for a Public Company's Board of Directors and Its Executive and Legal Team"[468]. It suggests that there are some measures that a company can take in order to assure a correct respect of the Duty of Oversight over Generative AI. First of all, every board member and executive team member should constantly have a correct understanding of what GenAI is, how does it work, its risks and, how the organizations uses and benefits from it. Therefore, a team of stakeholders for an additional oversight of GenAI may be useful and, members with expertise in AI could be added to the board. Another great suggestion provided by the article is the creation by the board and executive team of a written framework, for making policies regarding public disclosures in the context of GenAI usage, incidents, and standards for professionals to oversee those systems, in conformity with the Security and Exchange Commission directives. The understanding and continuous updating of legislation is also fundamental, together with the addressing of ethical standards for GenAI usage, development and deployment. In conclusion, Tiano recommends to entertain a close collaboration between boards and legal counsel to minimize GenAI risks. Legal professionals should be involved in the decision-making process to

[465] *See supra note 443.*
[466] *Id.*
[467] *See supra note 459.*
[468] *See supra note 431.*

offer guidance on regulatory compliance, risk mitigation and formulation of legal strategies related to GenAI[469].

Concerning other countries, the imposition of liability is someway similar to US. Talking about China, in December 2023 the National People's Congress revised and approved the sixth amendment to the Company Law of the People's Republic of China[470] , which entered in force in July 2024. It contributes with 112 newly added or revised articles, addressing significant aspects such as corporate governance, capital contribution and management responsibilities[471].

The imposition of liability is addressed by Article 147. It stipulates that the directors, supervisors and senior managers in order not to be held liable for damages, shall comply with the laws, administrative regulations and bylaw and, they shall bear the obligations of loyalty and diligence to the company[472].

The renewed obligations for directors, supervisors and senior managers are divided into the *Duty of Loyalty* and the *Duty of Diligence*. The first requires these key personnel to avoid conflicts of interest between their personal interests and those of the company, so they are prohibited from leveraging their positions to gain improper benefits. The *Duty of Diligence* instead, requires directors, supervisors, and senior managers to exercise reasonable care, by always prioritizing the company's best interests. Additionally, directors, supervisors, and senior managers are obliged to report their contracts and transactions to the company. The approval from the shareholders' meeting or from the board of directors is required and, must be obtained in accordance with the company's articles of association[473].

These regulations extend to close relatives of directors, supervisors, senior executives and to businesses under direct or indirect control of these individuals or of their close relatives. Moreover,

[469] *Id.*

[470] Zhonghua Renmin Gongheguo Gongsi Fa [Company Law of the People's Republic of China], Standing Committee of the National People's Congress, Dec. 29, 1993, in Zhonghua Renmin Gongheguo Fagui Haibian [Official Decree of the PRC], No. 59, 1 (1993).

[471] *See* RsA asia, *Fiduciary Duty in China's New Company Law* (2024), RSA ASIA, https://www.rsa-tax.com/single-post/fiduciary-duty-in-china-s-new-company-law.

[472] *See AI and directors' duties*, 2023 CBLJ 1.

[473] *See supra note 471.*

they cover any partiy involved in related-party relationships, who participate in contracts or transactions with the company[474].

If directors use Artificial Intelligence to make decisions and perform their duties causing harm to others, the company shall bear the corresponding compensation liability. Otherwise, if there is evidence that they have not fulfilled the relevant obligations of loyalty and diligence mentioned above, it can be considered that they have fault, negligence and violated their obligations as directors and, should consequently bear corresponding liability for damages. However, given the complex nature of AI and the difficulty in controlling technical risks by non-professionals, when it can be proven that the AI introduced to govern the company has significant defects, the manufacturer that develops it should compensate the company for the losses incurred due to the decisions made by the company based on the recommendations of the AI[475].

In Russia, the situation is a bit different. In July 2024, The Russian State Parliament (Duma) passed *Bill no. 512628-8*[476]. It requires AI developers operating within Experimental Legal Regimes (ELRs) to obtain civil liability insurance covering potential harm caused by AI, including damage to life, health or property. The Bill specifies insurance conditions such as minimum insured amounts and covered risks. Additionally, it requires ELR participants to maintain registers of personnel responsible for AI technology, who will be accountable in emergencies[477]. Indeed, under current state policy, responsibility for all consequences of AI systems is attributed to an individual or legal entity. And, in cases of harms caused by AI there can be applied either civil liability or criminal liability. The first applies if an individual, legal entity or their property is harmed. In that case, the person causing the harm must fully compensate the victim. This provision is universal and applies to all torts not

[474] *Id.*

[475] *See* Hao Xue , *Legal Regulation of Artificial Intelligence Directors under the Background of the Revision of China's New Company Law* (2024), RESEARCH GATE, https://www.researchgate.net/publication/382766555_Legal_Regulation_of_Artificial_Intelligence_Directors_under_the_Background_of_the_Revision_of_China's_New_Company_Law/fulltext/66abf611299c327096a3331d/Legal-Regulation-of-Artificial-Intelligence-Directors-under-the-Background-of-the-Revision-of-Chinas-New-Company-Law.pdf.

[476] Postanovleniia palat Federal’nogo Sobraniia [resolution of the State Duma] 2024, Bill No. 512628-8.

[477] *See* Data Guidance, *Russia: Duma passes bill on insuring civil liability from AI use* (2024), DATA GUIDANCE, https://www.dataguidance.com/news/russia-duma-passes-bill-insuring-civil-liability-ai .

explicitly regulated by law. The court will determine this on a case-by-case basis. Criminal liability instead, defines AI as a mean of committing crime, so in crimes committed using AI technologies, the Criminal law[478] provisions are fully applicable. When talking about AI systems, depending on the circumstances, it can be deemed responsible the AI developer, the AI user, the provider of AI services or the owner of exclusive rights to the AI[479].

In European Union instead, even though in 2022 it was presented a proposal for a possible AI liability Directive[480], in February 2025 the European Commission decided to abandon it. The decision to move on was proposed by the German Member of European Parliament Axel Voss, who told that the directive would have created unneeded regulation with the EU *AI Act*[481] in place. Also the Commission's President Ursula von der Leyen has endorsed this idea, by stating that in order to support AI market growth, a simple and unique rule would be more effective[482].

For this reason, for cases of harm caused by AI it is currently being applied the EU broader digital regulatory regime, including *GDPR*[483] and the *Digital Services Act*[484][485].

Following *GDPR*[486], the controller or the processor of an AI system has to provide compensation for the entire damage to any person who has suffered from the infringement of the *GDPR* directives. However, liable individuals, in order to pay the compensation, are entitled to recover from other relevant parties their respective part of responsibility. The *GDPR* clarifies that compensation may be recovered for both pecuniary and nonpecuniary losses. It states also that controllers and processors

[478] Ugolonyī Kodeks Rossiīskoī Federatsii [UK RF] [Criminal Code] (Russ.).
[479] *See Development of AI regulations in Russia*, 2025 ABLJ 1.
[480] See European Parliament, *Artificial Intelligence Liability Directive*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf
[481] *See supra note 69.*
[482] *See* Caitlin Andrews, *European Commission withdraws AI Liability Directive from consideration* (2025), IAPP, https://iapp.org/news/a/european-commission-withdraws-ai-liability-directive-from-consideration .
[483] *See supra note 71.*
[484] Regulation (EU) 2022/2065 of the European Parliament and of the Council of October 19,2022, on a single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), [OJ L 277, 27.10.2022] .
[485] *See supra note 482.*
[486] See supra note 71.

are exempt from liability if they are not responsible in any way possible for the event causing the damage[487].

Furthermore, the *Digital Services Act*[488] prohibits any general monitoring obligation from being imposed on online platforms and, holds a provider liable for illegal content only if by obtaining actual knowledge of the illegality they fail to rapidly remove or disable access to the content[489] .

4.2 AI in DAOs (Decentralized Autonomous Organizations) – Examining liability in decentralized corporate structures

Decentralized autonomous Organizations (DAOs) are a rapidly growing force in the crypto sphere, even though their legal status remains a mystery in some way[490].

DAOs are a type of joint enterprises that operate without a central command structure. Decisions are made through a consensus of the members towards a common goal. They are built on a complex web of smart contracts that determine the decision-making structure, which acts as the DAO constitution. It may be modified to suit the specific needs of the DAO. Voting rights are conferred by crypto coin ownership to shareholders and, unlike any traditional company, DAOs usually have minimal or no delegation of decision-making to an executive board. While some of them have committees to carry out various functions, these usually do not exercise high degrees of autonomy and only execute decisions of the majority[491].

[487] *See* Two Birds, *Remedies and liabilities,* TWO BIRDS, https://www.twobirds.com/-/media/pdfs/gdpr-pdfs/71--guide-to-the-gdpr--remedies-and-liabilities.pdf .

[488] *See supra note 484.*

[489] *See* Peter Church et al., *The EU Digital Services Act: A new era for online harms and intermediary liability* (2023), LINKLATERS, https://www.linklaters.com/it-it/insights/blogs/digilinks/2023/february/the-eu-digital-services-act---a-new-era-for-online-harms-and-intermediary-liability .

[490] *See* Chintan Dave, *Understanding DAOs and its Legal Liabilities* (2023), LINKEDIN, https://www.linkedin.com/pulse/understanding-daos-its-legal-liabilities-chintan-blockchain-trainer/ .

[491] *Id.*

Nowadays, they are becoming increasingly popular the disputes around crypto and metaverse companies, especially regarding intellectual property. Trademark, patent and copyright infringements are very common in the digital context. However, the main issue when talking about DAOs is always figuring out who to take action against and how to bring a claim [492].

A landmark example is the case *Samuels v. Lido*[493]. It is a ruling of utmost importance for DAOs, since through it, it was established that all DAO members, including large institutional backers, have to be considered legal partners. So, all members should be directly responsible for DAO's liabilities. In that trial, they were held liable the backers Paradigm, Andreessen Horowitz and Dragonfly. *Lido* ruling dismantled the concept of "entityless" that had usually been attributed to DAOs and, clarifies that these kinds of companies have to establish proper legal structures to protect their members , ensure long-term scalability and mitigate financial risks[494].

Similar legal arguments were used in cases against bSz DAO and Ooki DAO. Thus, reinforcing the urgent need for DAOs to adopt comprehensive legal structures that fully wrap their governance, community, and major assets[495].

For this purpose, in February 2025, a new modular and jurisdiction-neutral framework was introduced for DAOs: the *Harmony Framework*[496]. It guarantees DAOs a scalable legal architecture that balances decentralization with legal recognition. So, that way, those companies that are present in multiple jurisdictions are allowed to shield their members, assets and contributors from legal and financial risks[497].

The *Harmony Framework*[498] defines DAO as: DAO-Specific Entity (DSE). It is a special form of non-profit legal entity which recognizes all token holders as members, basing on their token holdings. It provides default limited liability for them, so that they are not held personally liable for the DAO

[492] *See* Sergey Ostrovskiy, *DAO 3.0: Ultimate Legal Structuring for DAOs in 2025 and Beyond* (2025), AURUM, https://aurum.law/newsroom/DAO-3-0-ultimate-dao-legal-structuring-in-2025-and-beyond .

[493] Samuels v. Lido DAO, No. 23-cv-06492-VC, 2024 WL 6782733 (N.D. Cal. Nov. 18, 2024).

[494] See supra note 492.

[495] *Id.*

[496] *See* DAO 3.0: *The Harmony Framework (2025),* DAOBOX, https://harmony.daobox.io/.

[497] *See supra note 492.*

[498] See supra note 496.

and its activities. It also allows for an effective management of legal, tax and financial risks[499]. In this set-up, high-risk activities can be separated from the DAO's governance and core property, thereby minimizing liability exposure and ensuring greater organizational resilience[500].

This method of asset and risk segregation reflects a well-established legal structuring approach used in traditional industries to safeguard assets and contain risks[501].

In short, the *Harmony Framework*[502] gives some key benefits to DAOs. First of all they have a distinctive legal identity from their members, DSE members and token holders get default limited liability protection as soon as they acquire tokens and, since the DSE structure is modular, highly scalable, and well defined, it can benefit of legally defined protections and regulations. Ultimately, their enormous advantage is jurisdiction neutrality, so the law applicable DAOs is valid in any country[503].

5. AI litigations and legal precedents

As policymakers and regulators work to create safe and trustworthy laws around Artificial Intelligence, dozens of AI-related lawsuits are simultaneously emerging in state and federal courts. All litigations and legal precedents that are being created and are likely to influence future laws about training data, copyright, data privacy and other issues[504].

Nowadays, most of the litigations are coming out of the copyright fight. Authors, artists, and institutions like The New York Times argue that they are under assault by powerful billion-dollars AI models like OpenAI's ChatGPT chatbot or Stability's Stable Diffusion image generator. However, as OpenAI officials pointed out in 2024 in the UK's House of Lords committee: "it would be

[499] *See* DAOBox, *Harmony TL;DR* (2025), DAOBox, https://harmony.daobox.io/harmony-tl-dr-a-5-min-read .

[500] *See* Sergey Ostrovskiy, *DAO 3.0: The Harmony Framework* (2025), DAObox, https://harmony.daobox.io .

[501] *Id.*

[502] See supra note 496.

[503] *See* supra note 500 .

[504] *See* Bruce Barcott, *AI Lawsuits Worth Watching: A Curated Guide*, 2024 Tech Policy Press 1.

impossible to train today's leading AI models without using copyrighted materials"[505]. And, it was curious to note that OpenAI did not even mention the possibility of paying to use license copyrighted materials at that time. Payment which is now being done via data deals with Reddit, The Financial Times, Vox Media, and others[506].

Moreover, another great part of lawsuits against AI is about the harms caused by matters such as algorithmic bias, liability, privacy harms and diffusion of false information[507], which are the ones that this document will mostly be analyzing.

In particular, the lawsuits which in recent times are increasingly involving Generative AI content have provided meaningful first looks of how US courts deal with matters such as invasion of privacy and property rights, copyright infringement, defamation and violations of state consumer protection laws[508].

Moreover, it has to be pointed out an emerging tendency, following which, courts have appeared reluctant to impose liability on AI developers and, have expressed skepticism of plaintiffs' rhetoric around AI's world-ending potential. There are also numerous complaints which lack in specific, factual and technical details that would be needed to proceed beyond the pleading stage[509]. National legislations have not been drafted to account for the challenges posed by AI, but still, global disputes and litigation trends surrounding AI are evolving rapidly as the technology becomes more pervasive across industries. This year it is expected to see AI lawsuits about defining liability for AI-driven decisions and algorithmic biases which prioritize higher classes[510].

[505] *See* Dan Milmo, *'Impossible' to create AI tools like ChatGPT without copyrighted material, OpenAI says* (2024), THE GUARDIAN, https://www.theguardian.com/technology/2024/jan/08/ai-tools-chatgpt-copyrighted-material-openai .

[506] *See supra note 504.*

[507] *Id.*

[508] *See* Amy Wong et al., *Recent trends in Generative Artificial Intelligence Litigation in the United States* (2023), K&L GATES, https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023.

[509] *Id.*

[510] *See* Dentons, *AI trends for 2025: Disputes and managing liability* (2025), DENTONS, https://www.dentons.com/en/insights/articles/2025/january/10/ai-trends-for-2025-disputes-and-managing-liability .

5.1 Key AI-related court cases (Lawsuits on AI bias, deepfake regulation, copyright infringement and AI personhood)

In this section it is presented a line of cases concerning some of the most debated themes regarding AI regulation nowadays. In particular, they will be analyzed lawsuits regarding AI personhood, AI bias, AI erroneous performance, deepfake regulations and copyright infringement.

Among the most relevant cases in AI corporate governance there is a landmark case which was useful to establish AI personhood and the rights that an AI developer can claim from their system. It is discussed whether an Artificial Intelligence software can be listed as the inventor on a patent application. The case at hand is *Thaler v. Vidal*[511], US (2022)[512].

Steven Thaler was the developer and owner of the Artificial Intelligent software DABUS (Device for the Autonomous Bootstrapping of Unified Science). In 2019, Thaler had filed two patent applications, naming DABUS as the sole inventor of them[513]. He wrote in the applications before the United States Patent and Trademark Office (USTPO) that the invention was generated by AI, instead of writing the inventor's last name[514]. It is important to note that the same process was done by Thaler in other dozen countries, for which other cases have emerged[515].

The USTPO denied Dr. Thaler's applications on the grounds that a machine can not qualify as an inventor[516]. After that, Thaler immediately sued the USTPO in the US District Court for the Eastern District of Virginia under the *Administrative Procedure Act*[517]. He claimed that his system was indeed the inventor of those and therefore should have been classified as such[518].

[511] Thaler v. Vidal, 43 U.S. (Fed. Cir. 2022).

[512] *See* Deidre M. Wells, *Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022) (Moore, Taranto, Stark)* (2023), STERNE KESSLER, https://www.sternekessler.com/news-insights/insights/thaler-v-vidal-43-f4th-1207-fed-cir-2022-moore-taranto-stark/.

[513] *See supra note 512.*

[514] *See* Monika J. Malek et al., *Thaler v. Vidal: Artificial Intelligence Inventions Create Real Issues* (2022), VEDDERPRICE, https://www.vedderprice.com/thaler-v-vidal-artificial-intelligence-inventions-create-real-issues.

[515] *Id.*

[516] *Id.*

[517] Va. Code Ann. §§ 2.2-4000 to -4033 (2024).

[518] See supra note 512.

However, the District Court concluded that the applications at hand lacked an inventor, because under the *Patent Act*[519] an "inventor" must be an "individual", so a natural person[520].

Dr. Thaler then appealed to the Federal Circuit to advocate for a broad interpretation of the term "individual", to include AI systems. He also pointed out that protecting inventions created by AI would be a big step forward for *Patent law*[521], which this way would have encouraged innovation and public disclosure. However, the Federal Circuit decided to go for a theoretical analysis, by focusing on the statutory interpretation of the *Patent Act*[522], by rejecting Thaler's argument[523]. It relied on a previous Supreme court ruling, in the case *Mohamad v. Palestinian Authority*[524][525], which stated that unless there is a Congress indication intending otherwise, the word "individual" in statutes, refers to human beings. To conclude, the Court guaranteed patent application to inventions made by human beings with the help of AI [526].

Consequently, in March 2023, Thaler decided to present a petition to the United States Supreme Court to ask for the review of the previous decision of the Federal Circuit's decision, arguing that the *Patent Act*[527] simply defines an inventor as one who invents, and therefore patent protections should be valid also for AI systems. But, the Supreme Court rejected his argument, by confirming that an inventor will continue to be referred as a human being in the United States[528].

It is interesting to point out that, while for now patent inventorship remains the domain of human beings, as AI continues to develop in the coming decades, the issue of AI inventorship will probably resurface[529].

[519] 35 U.S.C. (2023).
[520] See supra note 512.
[521] See supra note 519.
[522] 35 U.S.C. §§ 1–376 (2024).
[523] *See supra note 514.*
[524] Mohamad v. Palestinian Authority, 566 U.S. 449 (2012).
[525] *See* Ji Mao, *Revisiting AI Inventorship in Thaler v. Vidal* (2022), HOLAND & KNIGHT, https://www.hklaw.com/en/insights/publications/2022/10/revisiting-ai-inteventorship-in-thaler-v-vidal .
[526] *See supra note 512.*
[527] *See supra note 519.*
[528] *See* Akin, *Supreme Court Will Not Review United States Court of Appeals for the Federal Circuit's Decision in Thaler v. Vidal* (2023), AKIN GUMP, https://www.akingump.com/en/insights/ai-law-and-regulation-tracker/supreme-court-will-not-review-united-states-court-of-appeals-for-the-federal-circuits-decision-in-thaler-v-vidal .
[529] *See supra note 525.*

Another case that is ongoing, but that will be foundational for AI law is *The Authors Guild v. OpenAI*[530] (2023). It concerns a seriously hot topic nowadays: whether the training of an AI model on copyrighted data and the consequent creation of deepfakes constitutes fair use or infringement[531]. The Authors Guild is the US's oldest and largest organization of writers. In September 2023 it filed a complaint in the Southern District of New York to sue OpenAI in a class action. In December of the same year then, the Plaintiffs amended the class action to include Microsoft, the chief investor of OpenAI, by claiming that[532] the training of those LLMs could not have happened without Microsoft's financial and technical support[533].

OpenAI was accused on grounds of copyright infringement for using The Authors' voices, characters and stories to train ChatGPT, which in turn allowed users to create unauthorized sequels of their copyrighted works. Plaintiffs argue that OpenAI should have obtained a licensing agreement on their copyrighted works before using them, so they seek a permanent injunction against OpenAI, to prevent similar harms from reoccurring[534].

All 17 authors of the abovementioned copyrighted works seek damages for the lost opportunity to license them and[535], assert that OpenAI and Microsoft forced them into a position where they unknowingly helped their own market replacement[536].

Copyright infringement in particular, is regulated under *17 US Code §501*[537]. It sets forth a list of exclusive rights for copyright owners, including the rights of: making and distributing copies or phonorecords of their works and of preparing derivative works based on them[538].

So, even though the different plaintiffs allege different infringements, they all allege that ChatGPT's

[530] The Authors Guild v. OpenAI Inc. et al. , No. 1:23-cv-08292 (2023).

[531] *See* Michalsons, *Authors Guild et al. v OpenAI | Copyright Infringement*, MICHALSONS, https://www.michalsons.com/blog/authors-guild-v-openai-copyright-infringement/74945

[532] *See supra note 531.*

[533] *See* Stella Haynes Kiehn, *Plot Twist: Understanding the Authors Guild . OpenAI Inc Complaint*, 2024 Wash. J. L. 1.

[534] *Id.*

[535] *Id.*

[536] *See supra note 531.*

[537] 17 U.S.C. § 501 (2024).

[538] *See* Cornell Law School, *17 U.S. Code § 106 – Exclusive rights in copyrighted works,* https://www.law.cornell.edu/uscode/text/17/106#:~:text=The%20five%20fundamental%20rights%20that,stated%20generally%20in%20section%20106

ability to provide derivative works infringed on their copyrighted materials. For instance, plaintiff Martin claims that ChatGPT has generated unauthorized sequel of his work "Clash of Kings"[539][540]. All plaintiffs also complain about ChatGPT's function of reciting parts of their copyrighted works. However, it is worth noting that from the compilation of the lawsuit, the device has no longer used parts of the abovementioned copyrighted works[541].

Furthermore, a main issue posed by Stella Haynes Kiehn in her article[542] from Washington journal of law about this suit is that although it is certain that ChatGPT has produced infringing work, it has to be discovered whether OpenAI knowingly trained ChatGPT on copyrighted materials[543]. However, Open AI still claims that its actions were lawful and, for the purpose it made a declaration on a blog post about the case *The New York Times v. OpenAI*[544] (where OpenAI was accused to train its models with The New York Times' information) OpenAI maintains that according to established legal precedent, using copyrighted materials to train large language models or other AI datasets typically qualifies as fair use[545].

The Library Copyright Alliance (LCA) also supports this fair use argument, pointing at the history of Courts applying the *US Copyright Act*[546] to AI. They object that *Fair use* is a legal doctrine allowing to use copyright-protected works even without a license, for scopes of comment, parody or criticism. The Alliance focused on the precedent found in *Authors Guild v. Hatitrust*[547] and upheld in *Authors Guild v. Google*[548]. In the latter case, the US Court of Appeals for the Second Circuit declared that Google's operations on copyrighted books for digitalizing and analyzing them were indeed fair use. So, LCA argues that even though those cases did not concern GenAI, they still involved Machine

[539] George R.R. Martin, *A Clash of Kings* (1998).

[540] *See supra note 533*

[541] *Id.*

[542] *See supra note 533.*

[543] *Id.*

[544] The New York Times Co. v. Microsoft Corp. Et al., No. 1:23-cv-11195, 2024 WL 4102492 (S.D.N.Y. 2024).

[545] *See supra note 533.*

[546] 17 U.S.C. §§ 101–810 (2024).

[547] The Authors Guild, Inc. v. HathiTrust, 755 F.3d 87 (2d Cir. 2014).

[548] The Authors Guild, Inc. v. Google, Inc., 804 F.3d 202 (2d Cir. 2015).

Learning, so they can be used as legal precedents[549].

However, it has to be noted that plaintiffs have not questioned the development of GenAI and the training of it. They have only asserted that the defendants had no right to use the Authors' copyrighted works to train their models and, that they should have instead used works in the public domain or paid for the copyrighted ones. In fact, the complaint specifically recognizes that OpenAI's chief executive Sam Altman has told Congress that he shares plaintiffs' concerns[550].

However, the case is still ongoing and the decision from the District court is pending[551]. *Copyright infringement* in most jurisdictions is a heavy burden to prove. This is because determining if there's enough similarity between the original work and the alleged infringing work can be subjective and difficult to quantify. More so, proving that the alleged infringer had access to the original work is often required and, this can be challenging with generative AI tools such as ChatGPT and CoPilot which explore the whole Internet[552].

As AI chatbots become more powerful, the risk for these kinds of lawsuits will grow more and more[553].

Another relevant case in US is *State v. Loomis*[554] (2016). It is about another pressing issue nowadays: the reliance on AI systems to make judgements and, the consequent possible implications regarding AI bias.

The roots of this case go back to 2012, when the State of Wisconsin, charged Eric Loomis with five criminal counts related to a drive-by shooting in La Crosse. After some time, Loomis denied his participation in the shooting,but admitted that he had driven the same car involved in the accident later that evening. However, Loomis resulted guilty of two charges: "attempting to flee a traffic officer and operating a motor vehicle without the owner's consent"[555][556].

Meanwhile, as a part of the sentencing preparation, a Wisconsin Department of Correction officer

[549] *See supra note 533.*
[550] *Id.*
[551] *See supra note 531.*
[552] *Id.*
[553] *See supra note 533.*
[554] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
[555] Id.
[556] *See State v. Loomis*, 130 Harv. L. Rev. 1 (2017).

prepared a Pre-Sentence Investigation (PSI) report, which incorporated a COMPAS risk assessment. It is needed to estimate the risk of recidivism based on both an interview with the offender and information from the offender's criminal history. The Trial Court ultimately imposed a sentence of six years in prison followed by five years of extended supervision for Loomis[557]. Consequently, Loomis claimed that the Court's reliance on COMPAS risk assessment had violated his rights and thus, filed a motion for post-conviction relief in the Trial Court. In particular, the infringement of his rights was argued because those kinds of assessments, apart from benefiting of methodology secrecy, provide data relevant only to particular groups of people. So, Loomis argued his deprivation of receiving an individualized sentence based on accurate information. Loomis additionally stated on due process grounds that the court unconstitutionally considered gender at sentencing, by relying on a risk assessment that took gender into account. The trial court denied this motion and Loomis appealed, by posing in the end the issue to the Wisconsin Supreme Court[558]. Justice Ann Walsh Bradley rejected Loomis's due process arguments and found that the use of gender as a factor in the risk assessment served the nondiscriminatory purpose of promoting accuracy. Moreover, Loomis had not provided sufficient evidence that the sentencing court had actually considered gender. Also, a COMPAS report is able to use only publicly available data and, data brought by the defendant. So, in the end the Court concluded that Loomis could have verified the accuracy of the information used in sentencing in order to deny or explain them[559].

However, concerning individualization, Justice Bradley admitted that COMPAS provides only data on recidivism risk for groups similar to the offender. But she argued that that system is not the sole base for a decision, the Courts indeed have the discretion to disagree with the assessment when it is inappropriate[560].

Therefore, Justice Bradley alarmed judges to proceed with caution when using such assessments and,

[557] *Id.*

[558] *See supra note 556.*

[559] *See* Studicata, *State v. Loomis* (2016), STUDICATA, https://studicata.com/case-briefs/case/state-v-loomis/.

[560] *Id.*

prescribed both how to present them to Courts and to what extent they should be used. The Justice highlighted also that those risk scores must not be final on the incarceration or on the severity of the sentence. Furthermore, it was declared that PSIs that incorporate a COMPAS assessment must include written warnings for judges about the nature and meaning of COMPAS risk assessments[561].

So, in the end, the Supreme Court of Wisconsin held that the use of a COMPAS risk assessment in sentencing did not violate Loomis's due process rights if certain limitations and cautions were observed[562].

Another Judge, Justice Abrahamson agreed with the judgment. She pointed out that the Court had difficulties in understanding algorithmic risk assessments and that she would have required a record from it about the capabilities of the tool. Justice Abrahamson argued that the lack of understanding of COMPAS assessments was a significant problem and, for this reason the court needed all the help possible. With this declaration she aimed to show that the court was mistaken in thinking that as long as judges are informed about COMPAS's potential inaccuracy, they can discount appropriately[563].

In the end, the *Loomis* court's opinion suggests an attempt to temper the current enthusiasm for algorithmic risk assessments in sentencing. It encourages judicial skepticism on the value of risk assessments, which alone do little to tell judges how to behave[564].

Ultimately, the *Loomis* opinion failed to give an answer to why, given the risks, courts should still use such assessments. Indeed, even though in that case the Court alerted judges about the dangers of those, its prescription was unclear on how to actually alter judges' evaluations of the reports. The court's advisement is unlikely to create meaningful judicial skepticism, since it is does not consider the internal and external pressures on judges and the difficulties for them to use such assessments[565].

Another line of cases which demonstrates AI's long way ahead is the various lawsuits against DoNotPay. From these lawsuits it emerges that even though last years have been the breakthrough

[561] *Id.*

[562] See supra note 559.

[563] *Id.*

[564] *Id.*

[565] *Id.*

for Generative AI, the world is not ready to fully embrace its applications yet. The cases are about AI's ability to perform legal performance and consequently the liability conferred to its creators. The first case in these terms, is *MillerKing v. DoNotPay*[566], even though it was mostly inconclusive. In March 2023, an Illinois law firm, MillerKing, brought a class action against the company DoNotPay on behalf of all law firms in the United States, alleging false association and false advertising under the *Federal Lanham Act*[567] and Illinois State law[568].

The firm based its lawsuit on DoNotPay's affirmations, without having a license, to allow consumers to fight corporations, beat bureaucracy and sue anyone at the press of a button[569].

After then, the directors of the company moved to dismiss the lawsuit, asserting that MillerKing lacked standing to sue it in federal court. Their claim was accepted by the court on the ground that MillerKing had failed to establish standing because it had failed to allege that it has suffered any concrete injury[570].

Other lawsuits against DoNotPay were brought alleging mostly the same torts, but were either voluntary dismissed or finalized without a concrete reaching. They were for instance, *Faradian v. DoNotPay*[571] and *Lee v. DoNotPay*[572][573].

It all ended when The Federal Trade Commission in 2024 finalized an order requiring DoNotPay to stop making deceptive claims about the abilities of its AI chatbot. The robot was defined as an inadequate substitute for the expertise of a human lawyer. The company was held liable for not testing to what extent its AI lawyer was comparable to a human one and, for not hiring attorneys to evaluate the service. The AI software's claimed capabilities were to be able to generate legal documents and

[566] MillerKing, LLC v. DoNotPay, Inc., No. 3:23-CV-863-NJR, 2023 WL 702244059 (S.D. Ill. 2023).
[567] 15 U.S.C. §§ 1051 et seq.
[568] See Justia, *Illinois Law*, https://law.justia.com/illinois/
[569] *See* Bod Ambrogi, *In Case of 'Real Lawyers Against A Robot Lawyer', Federal Court Dismisses Law Firm's Suit Against DoNotPay for Unauthorized Law Practice* (2023), LAWSITES, https://www.lawnext.com/2023/11/in-case-of-real-lawyers-against-a-robot-lawyer-federal-court-dismisses-law-firms-suit-against-donotpay-for-unauthorized-law-practice.html .
[570] *Id.*
[571] Faradian v. DoNotPay, 123 F.4th 456 (9th Cir. 2023).
[572] Lee v. DoNotPay, 123 F.4th 456 (9th Cir. 2023).
[573] *See supra note 569.*

to give legal advice[574].

So, the final order required DoNotPay to pay $193,000 in monetary relief and to notify consumers who subscribed to the service between 2021 and 2023 about what happened. The order also prescribes the company not to advertise its service as being able to equate a real lawyer, unless being capable of proving it[575].

5.2 Legal controversies surrounding AI liability (Determining responsibility for AI – analyzed evidence)

In this section, they are presented two lawsuits which concern liability controversies and the extent to which responsibility is applied to AI.

The case at stand is *Megan Garcia v. Character Technologies, et al.*[576] (2024). It is a landmark case about the potential disruptive nature of AI and the liability of companies for AI errors, together with their negligence in making appropriate verifications before the launch of AI platforms. Character.AI is a platform powered by AI, which allows users to interact with AI-generated characters[577]. In October 2024, Megan Garcia filed a federal lawsuit claiming that the company was responsible for the death of her 14 years old son, Sewell Setzer III. The guy in question, had spent months talking to a chatbot on Character.AI before shooting himself to death due to a virtual conversation[578].

Garcia, represented by the Social Media Victims Law Center, alleged that Character.AI recklessly gives teenage users unrestricted access to lifelike AI companions, without properly safeguarding or

[574] *See* Federal Trade Commission, *FTC Finalizes Order with DoNotPay that Prohibits Deceptive 'AI Lawyer' Claims, Imposes Monetary relief, and Requires Notice to Past Subscribers*(2025), FTC, https://www.ftc.gov/news-events/news/press-releases/2025/02/ftc-finalizes-order-donotpay-prohibits-deceptive-ai-lawyer-claims-imposes-monetary-relief-requires.

[575] *See supra note 574.*

[576] Garcia v. Character Technologies, Inc., No. 6:24-cv-01903, 2024 WL [pinpoint citation] (M.D. Fla. 2024).

[577] *See* Social Media Victims Law Center, *Character.AI Lawsuits* (2025), SOCIAL MEDIA VICTIMS LAW CENTER https://socialmediavictims.org/character-ai-lawsuits/ .

[578] *Id.*

warning them, thus inferring negligence. Additionally, Garcia asserts that Character.AI deploys addictive design features to increase user engagement and steer vulnerable users toward intimate conversations. In particular, the inadequate measures to protect the general public set up by Character.AI are claimed to be especially defective for minors, whose brains have not reached full developmental maturity. Thus, exposing them to dangers like sexual exploitation and solicitation, child pornography, unlicensed therapy, dangerous power dynamics and chatbots that encourage self-harm and suicide[579].

Garcia declares that his son had developed a strong emotional attachment to the chatbot and that before the accident he had even began to isolate himself from the real world, eventually affecting his school performance. The mother argues that if Character.AI had warned users about the negative mental health effects of using the app, such as self-isolation, depression and suicide, this tragedy would not have happened[580].

In contrast, the declaration of 2023 of Noam Shazeer, the founder of Character.AI, was that the platform could be "super, super helpful to a lot of people who are lonely or depressed"[581]. So, not only has the app led to the suicide of a vulnerable teenage user, but its creator had also publicly hailed the app for unverified mental health benefits[582].

In her complaint Megan Garcia is seeking compensatory damages. She claims medical and funeral expenses, loss of companionship, mental anguish, emotional distress and loss of her son's future earnings potential. Garcia's attorneys have estimated these damages to exceed $5 million. Additionally, the lawsuit seeks punitive damages deriving from the platform's and the other defendants' conscious disregard for user safety, demonstrated by the lack of implementation of adequate safeguard measures for vulnerable minors. The complaint alleges that the defendants knew or should have known the potential psychological impacts of the AI technology. Furthermore, Garcia

[579] *See supra note 577.*

[580] *Id.*

[581] *See supra note 577.*

[582] *Id.*

requests injunctive relief to make Character.ai implement better age verification systems, better warning systems and content moderation protocols[583].

In similar cases in which social media platforms have caused mental health issues in youth, defendants have sought to evade liability through *Section 230 of the Communications Decency Act*[584] of 1996, which states that platforms can not be held liable for third-party content. However, recent lawsuits are increasingly claiming that when they are present addictive algorithms or harmful products, tech platforms should be held liable [585].

So, the question of law of this lawsuit is whether Character.AI content should be protected by *Section 230*[586], being an AI-generated content[587].

The defendants of this case do not include only Character Technologies, Inc. and Noam Shazeer, but they also comprise Daniel De Freitas Adiwarsana, Google LLC, and Alphabet Inc.. Together, they filed several motions seeking to end or pause the litigation. In particular, Character.ai filed a motion to compel arbitration, arguing that when the users agreed to the Terms of Service in creating accounts, those included a binding arbitration agreement stating that all disputes shall not be resolved by a court, but rather through final and binding arbitration. This means that an arbitrator and, not the court, must evaluate any issue concerning the arbitration agreement's validity. The company also addresses the plaintiffs' attempt to disaffirm the Terms of Service on behalf of their minor children, arguing that such disaffirmation is ineffective since the users at stand continue using the service[588].

Moreover, Google, Alphabet, Shazeer and De Freitas filed a joint motion to compel arbitration despite not being signatories to the Terms Of Service, by claiming the doctrine of *equitable estoppel*[589].

The doctrine of *equitable estoppel* is a legal defense that stops a party from asserting a right against

[583] *See* Kayne McGladrey, *Garcia v. Character.ai – Defendants File Motions to Compel Arbitration and Dismiss Claims* (2025), LINKEDIN, https://www.linkedin.com/pulse/garcia-v-characterai-defendants-file-motions-compel-kayne-mcgladrey-sdckc/ .
[584] 47 U.S.C. § 230 (2023).
[585] *See supra note 577.*
[586] See supra note 584.
[587] *See supra note 577.*
[588] *See supra note 583.*
[589] *Id.*

another when that right is based on misleading or deceptive behavior by the party claiming it[590]. Indeed plaintiffs' claims against them are intertwined with the claims against Character.ai and arise from the same alleged conduct. The non-signatory defendants argue that plaintiffs should treat all defendants as a single unit, since they are all providers of AI-powered chatbots[591].

Therefore, all defendants collectively submitted a motion to pause discovery until their motions to compel arbitration are resolved. They believe that a further scrutiny of Character.Ai would violate its right to arbitrate and would deprive it of benefitting from its arbitration agreements[592].

In these terms Kayne McGladrey, the CISO at Hyperproof, intervenes, by providing an analysis[593] about the possible implications of the case. He states that if the Court does not guarantee the motion to compel arbitration and, in turn lets the case proceed, it may be interpreted as an admission of insufficiency of the existing frameworks to address these kinds of harms[594].

Moreover, after this lawsuit, Regulators might impose stricter age verification protocols for AI systems capable of emotional engagement. Also, companies might face requirements to demonstrate the testing process for psychological safety of the AI systems and, they could be required to disclose known risks and limitations of their systems, particularly regarding emotional manipulation or harmful content generation[595].

This case have the potential to prompt legislators to develop specific liability frameworks for AI-related harms, thus clarifying the extent to which companies are responsible for their systems' outputs[596].

The court's handling of the arbitration will have far-reaching implications for future litigations involving AI companies and their potential liability for user interactions. This case could trigger significant regulatory scrutiny of AI businesses, particularly those developing conversational agents

[590] *See* Legal Information Institute, *estoppel in pais*, https://www.law.cornell.edu/wex/estoppel_in_pais .

[591] *Id.*

[592] *See supra note 583.*

[593] *Id.*

[594] *Id.*

[595] *Id.*

[596] *Id.*

accessible to minors. Indeed, currently, AI systems operate in a relatively unregulated environment, with companies largely self-policing through terms of service and content moderation practices[597]. The second lawsuit that may be pointed out in terms of liability, is *Mobley v. Workday*[598]. In this case, the plaintiff alleges that Workday's AI-powered applicant tools discriminate on the basis of race, age and disability, in violation of federal and state Anti-discrimination Laws[599]. This class action has the great potential to set precedent for AI vendor liability in hiring processes[600].

Mobley is a Black man of 40 years old who had anxiety and depression and, who holds a finance degree from Morehouse College. Between 2017 and 2024 he applied for over 100 jobs by using Workday's AI-based hiring tools, by being rejected every time. Mobley alleges that these AI systems incorporate illegal biases and rely on prejudiced training data, resulting in a disparate impact. Specifically, he contends that the AI could have: inferred his race from his graduation in an historically Black college, determined his age from the graduation year and, identified his mental disabilities through personality tests[601]. The key issue before the Court was whether Workday could be directly liable under *Title VII*[602] and other Federal Civil-rights laws[603].

Initially, the Court granted Workday's request to dismiss the motion, with leave to amend. But, following, the plaintiff filed the first amended complaint and, Equal Employment Opportunity Commission (EEOC) filed an amicus brief supporting the plaintiff's novel theories of direct AI vendor liability and urging the Court to deny the second motion to dismiss that Workday had requested [604].

[597] *Id.*
[598] Mobley v. Workday, Inc., No. 3:23-cv-00770-RFL, 2024 U.S. Dist. LEXIS 126336 (N.D. Cal. 2024).
[599] See Civil Rights Division, *Federal Protections Against National Origin Discrimination* (2000), US DEPARTMENT OF JUSTICE, https://www.justice.gov/crt/federal-protections-against-national-origin-discrimination-1 .
[600] *See* Annette Tyman, *Mobley v. Workay: Court Holds AI Service Providers Could Be Directly Liable for Employment* (2024), SETFARTH, https://www.seyfarth.com/news-insights/mobley-v-workday-court-holds-ai-service-providers-could-be-directly-liable-for-employment-discrimination-under-agent-theory.html .
[601] *See* HRWorks, *Implications of Mobley v. Workday* (2024), HRWORKS, https://hrworks-inc.com/industry-update/implications-of-mobley-v-workday/#:~:text=Between%202017%20and%202024%2C%20Mobley,resulting%20in%20a%20disparate%20impact.
[602] Civil Rights Act of 1964, Title VII, 42 U.S.C. § 2000e et seq. (2023).
[603] *See supra note 600.*
[604] *Id.*

The Court's decision was issued on July 12, 2024. It rejected the theory that Workday, the AI vendor, was an "employment agency" under federal law, finding that Workday's alleged activities did not meet the statutory definition of "procuring" employees for employers. Then, by analyzing the first amended complaint, it found no support for allegations that Workday was the entity recruiting or soliciting candidates. So that claim was dismissed[605].

While the Court's rejection of the "employment agency" theory of liability represents a partial rejection of the liability theories advanced by the plaintiff and the EEOC, it accepted the "agent" theory of liability. So, now AI vendors have a precedent to face direct liability for employment discrimination claims[606]. The Court indeed emphasized that Workday's customers, by using the platform, delegated their traditional function of rejecting or accepting candidates[607].

Workday argued that it was simply providing a tool to implement the employers' criteria. But, the Court asserted that Workday's software actively contributed to the decision-making process, by suggesting certain candidates for advancement while excluding others[608].

The Court also analyzed the allegation that Mobley received rejection emails almost immediately after submitting his application, which inferred a lack of review. But, even though the Court agreed that that this rapid rejection could be evidence of sole automation in the decision-making process, it rises doubts on whether such a fast rejection can simply be consistent with the usual rote criteria used by employers. So, it has to be verified to what extent the degree of automation and decision-making authority were relevant for the decision[609].

The Court drew a distinction between simple tools such as spreadsheet programs and email systems and Workday. It declared that Workday qualifies as an agent, since its tool performs a traditional hiring function of rejecting and accepting candidates at early stages through the use of artificial

[605] *Id.*

[606] *See supra note 600.*

[607] *Id.*

[608] *Id.*

[609] *Id.*

intelligence and machine learning[610].

Furthermore, the Court's opinion emphasized the importance of the *agency theory* in addressing potential enforcement gaps in anti-discrimination laws. Without the *agency theory*, the Court opined, no party could be held liable for this intentional discrimination[611].

Indeed, Agency theory describes the connection between principals and agents, where the principal depends on the agent to carry out business or financial tasks on their behalf and to act in the principal's best interests, setting aside any personal gain[612].

As a result, these claims will be subject to further scrutiny. Plaintiffs are likely to seek broad discovery into Workday's AI algorithms, their training data and the way these tools have been used in the hiring processes[613].

By allowing the plaintiff's *agency theory* to proceed, as supported by the EEOC in its amicus brief, the ruling would open the door for a significant expansion of liability for AI vendors in the hiring process, with potential far-reaching implications for both AI service providers and for employers using those tools[614].

6. Future legal challenges in AI deployment

Artificial Intelligence is reshaping many creative fields, decision-making processes and industries. It is influencing numerous sectors, such as healthcare, communication, transportation and entertainment, thus introducing unique challenges for existing legal systems[615].

[610] *Id.*
[611] *Id.*
[612] *See* Katie Kerpel, *What Is Agency Theory?* (2024), INVESTOPEDIA, https://www.investopedia.com/terms/a/agencytheory.asp .
[613] *See supra note 600.*
[614] *Id.*
[615] *See* Shari Davidson, *The Growth of AI Law: Exploring Legal Challenges in Artificial Intelligence*, 15 Nat. L. Rev. 1 (2025).

Traditional laws often fail to address every legal matter concerning AI systems. For this reason, a lot of times, because of the premature AI integration into business and daily life, there is the need for legal professionals with deep expertise in law and technology to manage the challenges and difficulties raised[616].

Since there are systems such as ChatGPT and DALL-E which generate creative works, there are still questions about who owns these outputs. For instance, the US Copyright Office recently adopted a policy declaring that AI-generated art cannot be copyrighted, following also the basis of the case *Thaler v. Vidal*[617]. Under *Copyright Office Policy*[618]: applicants for registration have a "duty to disclose the inclusion of AI-generated content in a work submitted for registration"[619].

Ownership disputes are likely to complicate business operations, since developers, organizations and users will always try to claim rights for AI-generated works and, attorneys will have to draft contracts to address specifically this matter[620].

Other possible issues arising with future AI developments concern data privacy. AI indeed depends on vast amounts of data to function, much of which are personal and sensitive. There may be applications of AI that cause gaps in privacy laws, since they were not designed taking into account current AI capabilities. Some examples may be AI-powered healthcare tools which analyze patient data to predict diseases and social media platforms which use algorithms to infer user preferences[621].

So, since AI systems process sensitive legal information, making them targets for cyber threats, law firms must implement robust cybersecurity measures to protect client data[622].

Another great and serious ethical challenge that is emerging more and more in recent years are the biases present in AI algorithms. Indeed, AI systems are trained basing on historical data which reflect

[616] *Id.*

[617] Thaler v. Vidal, 43 (Fed. Cir. 2022)**.**

[618] U.S. Copyright Office, Compendium of U.S. Copyright Office Practices § 101 (3d ed. 2021).

[619] *See supra note 615.*

[620] *Id.*

[621] *Id.*

[622] *See* World Lawyers Forum, *The Future of AI in Legal Practices: Opportunities & Challenges* (2025), WORLD LAWYERS FORUM, https://worldlawyersforum.org/articles/future-ai-legal-practice-opportunities-challenges/ .

societal inequalities, such as hiring algorithms that favor males over females or predictive policy tools which disproportionately target minority communities. In these cases it is unclear whether the blame should fall on developers, deployers or on those who provided the data. For now, attorneys are pushing for greater transparency in AI decision-making processes and for policies requiring regular audits of algorithms to identify and mitigate bias[623]. AI could perpetuate and even exacerbate preexisting discrimination in the legal system, so AI development must prioritize fairness and equity, necessitating ongoing vigilance to identify and address bias in AI applications[624].

Furthermore, as AI systems gain autonomy, determining liability for errors becomes increasingly complex. Current liability frameworks are not designed for these scenarios, so clear rules necessitate to be established, together with insurance policies that account for AI-related risks[625]. Moreover, since attorneys, lawyers and legal experts should provide for all those matters, also their training should be enhanced. They must be able to understand how an AI system works, interpret evolving regulations and address ethical implications. Some institutions are already trying to be prepared for these needs. For instance, the University of California, Berkeley offers targeted programs for legal practitioners through initiatives like the Berkeley Law AI Institute and the Berkeley AI Policy Hub[626].

In a declaration[627], the CEO of Paragon Tech, Inc., Jay McAllister, said that: “Attorneys who opt to ignore these developments will find themselves at an ever-increasing disadvantage when compared to those who embrace AI and seek to understand its mechanics and implications"[628] [629].

Overall, ethics plays a central role in AI law. The American Bar Association released its *Guidance for lawyers on the use of AI*[630] on July, 2024. Apart from ensuring compliance, it states that lawyers must advise clients on responsible AI use by all means, such as by promoting fairness, preventing

[623] *See supra note 615.*
[624] *See* Tshilidzi Marwala, *AI And The Law – Navigating The Future Together* (2024), UNU, https://unu.edu/article/ai-and-law-navigating-future-together .
[625] *See supra note 615.*
[626] *Id.*
[627] *Id.*
[628] *Id.*
[629] *See supra note 615.*
[630] *See* American Bar Association, *ABA issues first ethics guidance on a lawyer’s use of AI tools* (2024), ABA, https://www.americanbar.org/news/abanews/aba-news-archives/2024/07/aba-issues-first-ethics-guidance-ai-tools/ .

harm and aligning technology with societal values. For example, lawyers might propose policies aimed at enhancing the transparency of decision-making algorithms, thereby building trust between organizations and uses[631].

Another challenge is the impact of AI on employment and on the legal profession. While AI can create new opportunities and roles such as AI specialists and data analysts, there may be a negative impact on existing legal professionals[632].

Therefore, as AI continues to evolve, ongoing dialogue and collaboration between legal professionals, technologists and ethicists will be essential in shaping the future of legal practice and in ensuring that AI serves the best interests of justice and society[633].

6.1 AI potential in the future (Future legal and economic applications of AI)

As a recent research[634] conducted by Epoch AI highlights, the training of AI systems in recent years is expanding at a rate of approximately four times per year. It outpaces even some of the fastest technological expansions in history, such as the mobile phone adoption or the solar energy capacity installation. And, as the research reveals, assuming constant interest and investments in AI development, by 2030 it would be feasible to train models that exceed the current GPT- 4 scale. So, by the end of this decade there could possibly be drastic advances in the current Artificial Intelligence world [635].

This huge and sharp increase in AI potentialities may have a great impact in almost any sector,

[631] *See supra note 615.*

[632] *See* Shodh Sagar, *Artificial Intelligence and the Future of Legal Practice: Opportunities and Ethical Challenges*, 2 Indian JL 1 (2024).

[633] *Id.*

[634] *See* Jaime Sevilla et al., *Can AI Scaling Continue Through 2030?* (2024), EPOCH AI, https://epoch.ai/blog/can-ai-scaling-continue-through-2030 .

[635] *See* Jaime Sevilla et al., *Can AI Scaling Continue Through 2030?* (2024), EPOCH AI, https://epoch.ai/blog/can-ai-scaling-continue-through-2030 .

particularly in the legal one. AI indeed, even now, is already reshaping a lot how businesses process data, evaluate opportunities, manage risks, perform due diligences and evaluate M&As[636]. Also, in order to guess future applications of AI systems, it is fundamental to analyze first the key current trends. For instance, in recent years it is verifying a rise of agentic AI, so those systems capable of independently setting and executing complex tasks. As the entrepreneur Nell Watson notes in the Financial Times: these systems have the potential to "uncover key insights and patterns"[637], by analyzing vast amounts of financial data, market trends and reports at speeds far beyond human capabilities[638]. Additionally, a trend that is common across companies is the unofficial AI adoption. So even though company policies have not allowed the formal integration of AI systems in the business processes, people are already implementing them to streamline tasks. This demonstrates the huge recognized potential of AI tools[639].

Another event that is happening in recent times, is that costs of deploying AI systems are continuing to decrease, so foundational AI technologies can one day be made accessible to firms of all sizes[640]. However, a matter of great concern is that while AI is demonstrating to be able to deal with stable and structured environments, its ability to adapt to changing economic conditions is still in question. Many systems are trained on data reflective of specific contexts, such as periods of market prosperity, so their abilities during economic crises or even emerging markets are not verified[641].

Still, human oversight remains crucial to interpret AI outputs, and at least for now, should not be neglected[642].

As AI technology becomes more accessible and affordable, its widespread adoption is likely to shift from being a competitive edge for large corporations to a baseline expectation across industries. The focus is no longer on whether businesses should integrate AI, but on how to do so effectively, ensuring

[636] *See* Casimir Rajnerowicz, *AI in Due Diligence: What It Means for M&A and Beyond* (2024), V7, https://www.v7labs.com/blog/ai-due-diligence .

[637] *See supra note 636.*

[638] *Id.*

[639] *Id.*

[640] *Id.*

[641] *Id.*

[642] *Id.*

it supports and improves current operations rather than causing disruption[643].

A research conducted by Thomson Reuters about "How Generative AI is Shaping the Future of Law: Challenges and Trends in the Legal Profession"[644], highlights that nowadays lawyers are excited to implement Generative AI solutions. For instance, David Cohen, the senior director of the client service delivery McCarthy Tétrault, points out that his company in 2024 implemented CoCounsel, the professional-grade GenAI assistant. He says that the response about the strategic advantage provided by AI was very positive [645].

The coexistence of AI and law can produce a legal system more equitable, accessible and efficient. For example, a potential benefit for AI in law, as far as systems will be further developed, could be its capacity to improve the accessibility of justice. Indeed, tools powered by AI may increase the accessibility of legal information for those who can not afford legal representation. Therefore, when online dispute resolution will be perfectioned, it would be possible to offer economically viable substitutes for conventional litigation[646]. An early attempt of this, even though being a failure, was the legal chatbot DoNotPay, which tried to provide legal advice and assistance on a range of issues, from small claims to immigration matters[647].

The other opportunities presented by AI in legal practice are for sure its improved accuracy and consistency. They indeed help to the minimize human errors, increase efficiency and save costs, thanks to the ability of analyzing vast numbers of documents in a short amount of time[648].

Moreover, once AI will be safely developed and tested, it may be capable to properly handle risk management. AI is already reducing and avoiding human errors, so one day it may be able to ensure better compliance with legal standards and minimize the risks associated with inaccurate

[643] *Id.*

[644] See Thomson Reuters, *How Generative AI is Shaping the Future of Law: Challenges and Trends in the Legal Profession* (2025), THOMSON REUTERS, https://www.thomsonreuters.com/en-us/posts/innovation/how-generative-ai-is-shaping-the-future-of-law-challenges-and-trends-in-the-legal-profession/ .

[645] *Id.*

[646] *See supra note 624.*

[647] *See* Shodh Sagar, *Artificial Intelligence and the Future of Legal Practice: Opportunities and Ethical Challenges*, 2 Indian JL 3 (2024).

[648] *Id.*

documentation or oversight[649].

Another great AI potential, which as always will be available once AI will be further developed and tested, is the possibility to conduct legal and reliable research for lawyers. So, finding real legal cases to base on and navigating the various intricate legal landscapes[650].

The responsible use of AI in law in the future will require to further address ethical considerations such as privacy. Law firms will have to carefully control AI vendors and implement strong security measures for confidential client information. Indeed, the training of these technologies is one of the main ingredients for success[651].

AI's capacity to analyze data and offer insights grants it a relevant place in the legal industry. Still, it is not intended to replace lawyers, instead it should be perceived as an advanced tool to amplify and improve legal professions. A robotic courtroom does not embody the future of law, which instead, will involve a balanced integration of AI and human intellect. In this scenario, AI would concentrate on data-intensive tasks, while humans will focus on developing strategic tactics and negotiation skills[652].

6.2 The future of AI in corporate law – How liability, compliance and governance may evolve

Regulation on AI, being this technology a completely new challenge, is trying to adapt to the new environment and act accordingly. A main problem as of today is still the lack of a global comprehensive legal framework. So that States like Russia, which have recently entered the environment, are not covered for all aspects, like data protection, risks of profiling and

[649] *See supra note 622.*
[650] *See* Bernice Melvin, *The future of Artificial Intelligence and legal careers* (2024), SMART LAWYER, https://nationaljurist.com/smartlawyer/the-future-of-artificial-intelligence-and-legal-careers/ .
[651] *See* NexLaw.AI, *Navigating the Future of AI and Law*, https://www.nexlaw.ai/the-future-of-ai-and-law/ .
[652] *See supra note 650 .*

discrimination[653]. However, the problem is not only for emerging countries in terms of AI, but it also characterizes giants such as US and EU[654].

Talking about US, its main impediment is that while technology is advancing at a fast rate, AI legislation is still slow and fragmented. And furthermore, the recent change of presidency has destabilized the order[655]. As Ryan Calo, law professor at University of Washington has said last year: "The US AI governance landscape right now is like a scattered jigsaw puzzle – bits and pieces everywhere that don't quite fit together"[656]. All this fragmentation derives from US division of powers between federal and state governments. Many key AI applications intersect with traditional state domains like education, healthcare, transportation, and law enforcement[657].

Moreover, another problem in US regulation, according to the AI researcher Gary Marcus, is that "Self-regulation is important, but it's not sufficient"[658]. Clear rules are needed[659]. US need to shift from a reactive, fragmented approach to a more proactive and coordinated one. This will require a greater emphasis on multi-stakeholder collaboration, thus bringing together government, industry, academia and civil society, to craft flexible yet robust AI governance frameworks[660].

However, recently, the US were able to take a step forward in AI regulation with the *Take It Down Act*[661]. On April 2025, the House of representatives passed the first major law regarding AI-induced harm. This Bill criminalizes non-consensual deepfake porn and requires platforms to take down such material. The Bill aims at discouraging AI-created illicit imagery and all those practices exposing users to inappropriate content[662].

[653] *See* DataGuidance, *Russia: Current status and development of AI regulations* (2024), DATA GUIDANCE, https://www.dataguidance.com/opinion/russia-current-status-and-development-ai .

[654] *See* White & Case, *AI Watch: Global regulatory tracker – United States* (2025), WHITE & CASE, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states .

[655] *Id.*

[656] See supra note 654.

[657] *Id.*

[658] *Id.*

[659] *Id.*

[660] *Id.*

[661] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act, Pub. L. No. 119-12, 139 Stat. 102 (2025).

[662] Andrew r. Chow, *Inside the First Major U.S. Bill Tackling AI Harms – and Deepfake Abuse*, 2025 Time 1.

Even though US have tried to make progress in AI regulation, a lot of challenges still remain. For instance, there is still the problem of liability for AI errors, as it has emerged from *Garcia v. Character.Ai*[663], which has not been ruled yet[664]. Additionally, from the case The *Author's Guild v. OpenAI*[665], it emerges that also the matter of copyright infringement is not so clear when talking about chatbots[666].

However, similar problems arise almost in all other jurisdictions. In China for instance, there are challenges with data protection. So, the problem of how to enforce transparent AI decision-making and data privacy. In China, a proactive approach to governance and risk management would be essential for businesses and regulators[667].

In European Union instead, there has been taken great and concrete moves towards AI regulation by enacting the EU *AI Act*[668]. However, the Yale Journal of Law & Technology proposes an interesting analysis[669] conducted by Sandra Watcher about the limits of the *Act*. First of all, it criticizes the *Act*'s decision not to ban systems such as those that perform biometric categorization. So, those systems that identify people in public spaces. It is indeed well established that remote biometric identification has abysmal accuracy rates (returning false matches some 80 percent of the time). Moreover, it claims that the list of high-risk applications is not complete. So, areas such as AI in finance and trading and specific consumer-facing applications, such as chatbots and pricing algorithms, are not considered, even though they are posing a huge risk for society. This is paired with the lack of standing for

[663] Garcia v. Character Technologies*, Inc.*, No. 6:24-cv-01903-ACC-UAM, 2025 WL 1461721 (M.D. Fla. 2025).
[664] *See supra note 583.*
[665] The Authors Guild v. OpenAI Inc.*,* No. 1:23-cv-08292 (S.D.N.Y. 2023).
[666] *See* Michalsons, *Authors Guild v OpenAI | Copyright Infringement*, https://www.michalsons.com/blog/authors-guild-v-openai-copyright-infringement/74945.
[667] *Charting a course with AI* regulation, 2025 IBLJ 1 .
[668] *See supra note 69.*
[669] *See* Sandra Watcher, *Limitation and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*, 26 YJoLT 5 (2024).

complete liability framework[670].

For AI, the path ahead is still long, but in the meantime, countries are trying to be updated.

7. Conclusion

After the various analysis and speculations done in this document, it is possible to notice that a lot of countries have made many efforts towards regulating AI. It is a technology which is introducing increasingly important changes in our today's world and, for this reason, people and governments are not always prepared. Europe is trying to control the situation by proposing a stringent approach, US on the contrary is trying to embrace innovation and, China and Russia, while being overall oriented to the reaching of specific guidelines, are trying to stay open. However, even with all the regulations, measures and initiatives enacted in the last years, AI ruling still remains a challenge. Artificial Intelligence indeed develops at an unprecedented speed and, while legislators face the difficulties raised last year, there are always new ones being posed. In conclusion, AI regulation is still incomplete on a global level. The challenges presented everyday outweigh the possibilities of governments to address them. It is not so clear whether the best approach to be kept is to deregulate as US is trying to do, or to enhance stringent measures as Europe has done. But, the clear thing is that great strides are being made and, if all challenges are accurately revised and furtherly evaluated before adoption, this could only go better.

Arianna Tosti

[670] *Id.*

References

- Akash Takyar & LeewayHertz, *AI Use Cases & Applications Across Major industries*, A HACKETT GROUP COMPANY, https://www.leewayhertz.com/ai-use-cases-and-applications/ .
- Alex Singla et al., *The State of AI: How organizations are rewiring to capture value* (2025), QUANTUMBLACK AI BY MCKINGSEY, https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai#/ .
- Adib Bin Rashid et al., *AI revolutionizing industries worldwide: a comprehensive overview of its diverse application*, 7 Hybrid Advances 2 (2024).
- Lexin Legal Law, *The Legal Future: Artificial Intelligence And Corporate Law (2025), MONDAQ,* https://www.mondaq.com/turkey/corporate-governance/1566104/the-legal-future-artificial-intelligence-and-corporate-law
- J.P Morgan Chase, *Omni Means "All"*, J.P. MORGAN CHASE, https://www.jpmorgan.com/technology/news/omni-ai.
- Rossana Miranda, *Ecco Vital, il primo robot consigliere di amministrazione*, 2014 Formiche 1.
- Philipp Rosenauer et al., *Artificial Intelligence Revolutionising corporate legal departments*, PWC, https://www.pwc.ch/en/insights/regulation/ai-revolutionising-corporate-legal-departments.html
- Bloomberg Law, *Can AI Write Legal Contracts?* (2024), BLOOMBERG LAW, https://pro.bloomberglaw.com/insights/technology/can-ai-write-legal-contracts/#contract-automation-tools
- Virtasant, *AI Contract Management: 80% Time Savings in Legal Work* (2025), ENTERPRISE AI TODAY, https://www.virtasant.com/ai-today/ai-contract-mangement-legal .
- Erin Walker, *AI Contract Drafting & Automation Tools for Lawyers* (2025), CLIO BLOG, https://www.clio.com/blog/ai-contract-drafting-and-automation/.
- Cimphony, *Top 10 AI Legal Drafting Tools 2025: Features & Pricing* (2025), CIMPHONY, https://www.cimphony.ai/insights/top-10-ai-legal-drafting-tools-2024-features-and-pricing .
- Gartner, *Mergers and Acquisitions (M&A)*, GARTNER, https://www.gartner.com/en/finance/glossary/mergers-and-acquisitions-m-a- .
- Redcliffe Training, *AI in M&A: How It's Changing Mergers & Acquisitions* (2024), REDCLIFFE, https://redcliffetraining.com/blog/ai-in-manda.
- Casimir Rajnerowicz, *AI in Due Diligence: What It Means for M&A and Beyond* (2024), V7 LABS, https://www.v7labs.com/blog/ai-due-diligence.
- Gabby MacSweeney, *The top 7 AI tools for M&A due diligence* (2025), LEGALFLY, https://www.legalfly.com/post/the-top-7-ai-tools-for-m-a-due-diligence.
- Bob Dillen, *How AI transforms document review in eDiscovery*, KPMG, https://kpmg.com/ch/en/insights/cybersecurity-risk/e-discovery.html .
- Gabriel MacSweeney, *The best AI tools for legal research in 2025* (2025), LEGALFLY, https://www.legalfly.com/post/best-ai-tools-for-legal-research-in-2025#:~:text=AI%20can%20deliver%20tailored%20analyses,need%20when%20you%20need%20it
- Bloomberg Law, *Can AI do legal research?* (2024), BLOOMBERG LAW, https://pro.bloomberglaw.com/insights/technology/can-you-use-ai-for-legal-research/ .
- Mata v. Avianca, Inc., 1:2022cv01461 U.S 1 (2023).
- Benjamin Weiser, *Here's What Happens When Your Lawyer Uses ChatGPT,* 2023 NY Times 1.

- Faiz Surani et al., *AI on Trial: Legal Models Hallucinate in 1 out of 6 (or More) Benchmarking Queries* (2024), STANFORD UNIVERSITY HUMAN-CENTERED ARTIFICIAL INTELLIGENCE, https://hai.stanford.edu/news/ai-trial-legal-models-hallucinate-1-out-6-or-more-benchmarking-queries .
- Ashley Hallene et al., *Using AI for Predictive Analytics in Litigation* (2024), AMERICAN BAR ASSOCIATION, https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2024-october/using-ai-for-predictive-analytics-in-litigation/
- Jane Wakefield, *AI predicts outcome of human rights cases (2016),* BBC, *https://www.bbc.com/news/technology-37727387* .
- Amy Swaner, *Using AI to Predict Legal Outcomes: A Powerful New Tool for Lawyers* (2024), AI FOR LAWYERS, https://aiforlawyers.substack.com/p/using-ai-to-predict-legal-outcomes .
- Dan, *AI-Powered Legal Case Outcome Prediction: Transforming Legal Practice* (2025), PRE-DICTA, https://www.pre-dicta.com/ai-powered-legal-case-outcome-prediction-transforming-legal-practice/#:~:text=These%20predictive%20analytics%20enable%20attorneys,streamline%20litigation%2C%20and%20enhance%20advocacy
- Katie Shonk, *AI Mediation: Using AI to Help Mediate Disputes* (2025), DAILY BLOG, PROGRAM ON NEGOTIATION - HARWARD LAW SCHOOL , https://www.pon.harvard.edu/daily/mediation/ai-mediation-using-ai-to-help-mediate-disputes/ .
- EY Global, *How to navigate global trends in Artificial Intelligence regulation* (2024), EY GLOBAL, https://www.ey.com/en_gl/insights/ai/how-to-navigate-global-trends-in-artificial-intelligence-regulation.
- Anand Kumar et al., *AI and Business Law: Navigating New Frontiers*, 67 Calif. Manag. Rev. 1 (2024).
- *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (Artificial Intelligence Act), 2024 O.J. (L 2024/1689).
- Timo Gaudszun et al., *AI Watch: Global regulatory tracker – European Union* (2025), WHITE & CASE, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-european-union.
- *Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation), 2016 O.J. (L119).
- Exabeam, *The Intersection of GDPR and AI and 6 Compliance Best Practices,* EXABEAM, https://www.exabeam.com/explainers/gdpr-compliance/the-intersection-of-gdpr-and-ai-and-6-compliance-best-practices/#:~:text=GDPR%20defines%20the%20requirement%20for,grounds%20of%20“legitimate%20interest
- Tania Goncalves, *The AI Act: Europe's Human Rights Contradiction Militarizing AI in the Name of Defense – The Human-Centric Illusion* (2025), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5158906
- Jon Chun et al., *Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US* (2024), ARXIV – CORNELL UNIVERSITY, https://arxiv.org/abs/2410.21279ù

- European Council – Council of European Union, *Artificial Intelligence Act ,* Council of European Union*,* https://www.consilium.europa.eu/en/policies/artificial-intelligence/
- Finextra, *What is the EU AI Act? Understanding Europe's first regulation on artificial intelligence* (2023), Finextra, https://www.finextra.com/the-long-read/847/what-is-the-eu-ai-act-understanding-europes-first-regulation-on-artificial-intelligence
- Brazil's Chamber of Deputies, *Bill No. 21-A/2020 (2020),* Derechos Digitales, *https://www.derechosdigitales.org/wp-content/uploads/Brazil-Bill-Law-of-No-21-of-2020-EN.pdf .*
- *See* Melissa Heikkilä, *Brazil's AI law – US takes a risk-based approach – Social scoring* (2021), POLITICO, https://www.politico.eu/newsletter/ai-decoded/brazils-ai-law-us-takes-a-risk-based-approach-social-scoring/
- *European Declaration on Digital Rights and Principles for the Digital Decade*, 2023/C 23/01 O.J. (C23) 1 (EU).
- AI & Partners, *EU AI Act: Trustworthy AI for the Digital Decade* (2025), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5147156
- OECD, *AI Principles*, OECD, https://www.oecd.org/en/topics/ai-principles.html .
- Shaping Europe's digital future, *AI Innovation Package*, Digital Strategy EU, https://digital-strategy.ec.europa.eu/en/factpages/ai-innovation-package
- Shaping Europe's digital future, *AI Factories*, Digital Strategy EU, https://digital-strategy.ec.europa.eu/en/policies/ai-factories .
- Shaping Europe's digital future, *Coordinated Plan on Artificial Intelligence*, Digital Strategy EU, https://digital-strategy.ec.europa.eu/en/policies/plan-ai .
- Shaping Europe's digital future, *AI Pact*, Digital Strategy EU, https://digital-strategy.ec.europa.eu/en/policies/ai-pact .
- European Commission, *AI Act,* Shaping Europe's digital future, *https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai*
- EU Artificial Intelligence Act, *High-level summary of the AI Act* (2024), EU Artificial Intelligence Act, https://artificialintelligenceact.eu/high-level-sum.mary/
- EU Artificial Intelligence Act, *Recital 24*, EU Artificial Intelligence Act, https://artificialintelligenceact.eu/recital/24/#:~:text=An%20AI%20system%20placed%20on,entity%20carrying%20out%20those%20activities
- *Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC*, 2019 O.J. (L 130) 92.
- *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (Artificial Intelligence Act), Chapter II Art. 5, 2024 O.J. (L 2024/1689).
- *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (Artificial Intelligence Act), Chapter III Art. 6, 2024 O.J. (L 2024/1689).
- *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (Artificial Intelligence Act), Art. 8-17, 2024 O.J. (L 2024/1689).

- *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (Artificial Intelligence Act), Chapter V, 2024 O.J. (L 2024/1689).
- *Regulation (EU) No. 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828* (Artificial Intelligence Act), Chapter VI , 2024 O.J. (L 2024/1689).
- European Parliament, *EU AI Act: first regulation on artificial intelligence* (2023), TOPICS EUROPEAN PARLIAMENT, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.
- La Quadrature du Net, *WITH THE AI ACT ADOPTED, THE TECHNO-SOLUTIONIST GOLD-RUSH CAN CONTINUE* (2024), LA QUADRATURE DU NET, https://www.laquadrature.net/en/2024/05/22/with-the-ai-act-adopted-the-techno-solutionist-gold-rush-can-continue/ .
- Wikipedia, *Artificial Intelligence Act*, WIKIPEDIA, https://en.wikipedia.org/wiki/Artificial_Intelligence_Act#:~:text=On%2021%20April%202021%2C%20the,and%20Parliament%20concluded%20an%20agreement .
- Tania Goncalves, *The AI Act: Europe's Human Rights Contradiction Militarizing AI in the Name of Defense – The Human-Centric Illusion* (2025), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5158906 .
- Tatevik Davtyan, *The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained (*2024), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4954290 .
- White & Case, *AI Watch: Global regulatory tracker – United States* (2025), WHITE & CASE, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states .
- Software Improvement Group, *AI Legislation in the US: A 2025 Overview* (2025), SOFTWARE IMPROVEMENT GROUP, https://www.softwareimprovementgroup.com/us-ai-legislation-overview/#:~:text=In%20the%20United%20States%2C%20the,Trump%20in%20his%20first%2Dterm
- *John S. McCain National Defense Authorization Act for Fiscal Year 2019,* Pub. L. No. 115-232 (2018).
- *National Artificial Intelligence Initiative Act of 2020*, Pub. H.R. 6216 (2019-2020).
- *AI in Government Act of 2020*, H.R. 2575 (2019-2020).
- *Advancing American AI Act*, S.1353 (2021-2022).
- *CHIPS and Science Act*, H.R. 4346 (2021-2022).
- *Countering Human Trafficking Act of 2021*, S. 2991 (2021-2022).
- *Algorithmic Accountability Act of 2023*, S. 2892 (2023-2024).
- *Expressing support for Congress to focus on artificial intelligence*, H. Res. 66 (2023-2024).
- *Amending House Resolution 211 to ensure that days occurring during the first session of the One Hundred Nineteenth Congress constitute calendar days for purposes of section 202 of the National Emergencies Act (50 U.S.C. 1622) with respect to a joint resolution terminating a national emergency declared by the President on February 1, 2025.* H. Res. 304 (2025-2026)
- *Stop Spying Bosses Act*, S.262 (2023-2024).

- *American Data Privacy and Protection Act*, H.R. 8152 (2021-2022).
- *SAFE DATA Act*, S. 2499 (2021-2022).
- 118th Congress*, House Bipartisan Task Force on Artificial Intelligence Delivers Report (2024),* COMMITTEE ON SCIENCE SPACE AND TECHNOLOGY, *https://science.house.gov/2024/12/house-bipartisan-task-force-on-artificial-intelligence-delivers-report* .
- *Artificial Intelligence Research, Innovation, and accountability Act of 2024*, S. 3312 (2023-2024).
- *Consumer Protections for Artificial Intelligence Concerning consumer protections in interactions with artificial intelligence systems*, SB24-205 (2024).
- See NIST, *AI Risk Management Framework* (2023), NIST, https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook .
- Illinois Supreme Court, *Illinois Supreme Court Announces Policy on Artificial Intelligence*, ILLINOIS COURTS, https://www.illinoiscourts.gov/News/1485/Illinois-Supreme-Court-Announces-Policy-on-Artificial-Intelligence/news-detail/ .
- *740 ILCS 14*, (2008)
- *Defending Democracy from Deepfake Deception Act of 2024* A.B. No. 261 (2024).
- *Use of Likeness: Digital Replica Act,* A.B. No. 1836 (2025).
- *California AI Transparency Act,* S.B. No. 942 (2023-2024)
- *Generative Artificial Intelligence: Training Data Transparency Act*, A.B. 2013 (2023-2024).
- *California Consumer Privacy Act* (2024), ROB BONTA ATTORNEY GENERAL, HTTPS://OAG.CA.GOV/PRIVACY/CCPA .
- *See* Joseph. R. Biden, Jr., *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), FEDERAL REGISTER, https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence
- White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (2022), WH.GOV, https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/.
- Yannic Mahé, *Divergent Paths: Comparing AI Regulation in the US, EU, and China* (2024), LINKEDIN, https://www.linkedin.com/pulse/divergent-paths-comparing-ai-regulation-us-eu-china-yannick-mahé-ztlre/ .
- Executive Office of the President National Science and Technology Council Committee on Technology, *Preparing for the Future of Artificial Intelligence* (2016), OBAMA WHITE HOUSE, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.
- *AI Accountability Policy Repor*t (2024), NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report .
- *Defense Production Act*, Pub. L. 81-774 (1950).
- Ken D. Kumayama et al., *US Federal Regulation of AI Is Likely To Be Lighter, but States May Fill the Void* (2025), SKADDEN, https://www.skadden.com/insights/publications/2025/01/2025-insights-sections/revisiting-regulations-and-policies/us-federal-regulation-of-ai-is-likely-to-be-lighter.
- Executive Office of the President Office of Management and Budget, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (2024), WHITE HOUSE, https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf .

- U.S. Department of the Treasury, *Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector* (2024), HOME TREASURY, https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf
- Joseph R. Biden, Jr., *Executive Order 14141—Advancing United States Leadership in Artificial Intelligence Infrastructure* (2025), THE AMERICAN PRESIDENCY PROJECT, *https://www.presidency.ucsb.edu/documents/executive-order-14141-advancing-united-states-leadership-artificial-intelligence*
- Joseph R. Biden, Jr., *Executive Order- 14144-Strenghtening and promoting innovation in the Nation's cybersecurity* (2025), FEDERAL REGISTER, https://public-inspection.federalregister.gov/2025-01470.pdf
- Donald J. Trump, *Removing Barriers to American Leadership in Artificial Intelligence* (2025), THE WHITE HOUSE, https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/
- Department of Health and Human Services, *Guidance for Regulation of Artificial Intelligence Applications* (2020) , https://www.hhs.gov/sites/default/files/department-of-health-and-human-services-omb-m-21-06.pdf .
- Ken D. Kumayama et al., *US Federal Regulation of AI Is Likely To Be Lighter, but States May Fill the Void* (2025), SKADDEN, https://www.skadden.com/insights/publications/2025/01/2025-insights-sections/revisiting-regulations-and-policies/us-federal-regulation-of-ai-is-likely-to-be-lighter.
- Mattew Kirk et al., *Key Insights on President Trump's New AI Executive Order and Policy % Regulatory Implications* (2025), SQUIRE PATTON BOGGS, https://www.squirepattonboggs.com/en/insights/publications/2025/02/key-insights-on-president-trumps-new-ai-executive-order-and-policy-regulatory-implications
- Chris Miller, *Chip War: the fight for the world's most critical ideology* (2022).
- Billy Perrigo, *How Trump's Tariffs Could Make AI Development More Expensive*, 2025 TIME 1.
- Epoch AI, *LLM Inference prices have fallen rapidly but unequally across tasks (*2025), EPOCH AI, https://epoch.ai/data-insights/llm-inference-price-trends .
- Anna Sytnik, *Russia and China: Development of Artificial Intelligence in Eurasia* (2025), VALDAI DISCUSSION CLUB, https://valdaiclub.com/a/highlights/development-of-artificial-intelligence-in-eurasia/
- Kaspersky AI Security Team, *AI Regulation in Russia* (2024), KASPERSKY, https://ai-cert.kaspersky.com/ai-regulation-ru.html#:~:text=AI%20regulation%20in%20Russia%20at,of%20the%20Russian%20Federation%20No
- *Development of AI regulations in Russia*, 2025 CBJ
- Christy Lee, VOA, *Russia turns to China to step up AI race against US* (2025), VOA, https://www.voanews.com/a/russia-turns-to-china-to-step-up-ai-race-against-us/7931829.html .
- Anton Vasiliev et al., *Ethical and legal aspects of the use of artificial intelligence in Russia, EU, and the USA: comparative legal analysis 2019 Redalyc 16.*
- Альянс в сфере искусственного интеллекта, *A Commission on AI Ethics has been established in Russia* (2022), https://a-ai.ru/?page_id=1699&lang=en#:~:text=It%20was%20created%20at%20the,work%20together%20to%20implement%20it.
- *Federal Law of the Russian Federation*, 2021, No. 258-FZ.
- Oksana Mamima et al., *Experimental legal regimes for digital innovation and a special regulation mechanism: new concepts of russian legislation and first projects* (2021), SHS

WEB OF CONFERENCES, https://www.shs-conferences.org/articles/shsconf/pdf/2021/17/shsconf_mtde2021_02009.pdf.

- Stip Compass, *Federal Law "On Experimental Legal Regimes in the Field of Digital Innovation in Russia"* , STIP OECD, https://stip.oecd.org/stip/covid-portal/policy-initiatives/covid%2Fdata%2FpolicyInitiatives%2F944
- *Resolution of the Government of Russian Federation*, 2020, No. 1618.
- Gary E.Murphy et al., *Russia Adopts Law on Regulatory Sandboxes* (2020), DEBEVOISE & PLIMPTION, https://www.debevoise.com/insights/publications/2020/09/russia-adopts-law-on-regulatory-sandboxes .
- *Concept for the Regulation of Artificial Intelligence and Robotics,* ICT MOSCOW, *https://ict.moscow/en/news/concept-for-the-regulation-of-artificial-intelligence-and-robotics-until-2024-has-been-approved/*
- *See Decree of the President of the Russian Federation On the Development of Artificial Intelligence in the Russian Federation,* (2019), CSET, https://cset.georgetown.edu/wp-content/uploads/Decree-of-the-President-of-the-Russian-Federation-on-the-Development-of-Artificial-Intelligence-in-the-Russian-Federation-.pdf
- *Federal Law On Advertising*, 38-FZ (2025).
- Postanovleniia palat Federal'nogo Sobraniia [resolution of the State Duma] 2024, Bill No. 512628-8.
- Digital Policy Alert, *Russia: Passed Bill establishing Digital Innovation and AI in Experimental Legal Regimes(Bill No. 512628-8)* (2024), DIGITAL POLICY ALERT, https://digitalpolicyalert.org/event/21208-passed-bill-establishing-digital-innovation-and-ai-in-experimental-legal-regimes-bill-no-512628-8 .
- BRICS Competition- Law & Policy Centre, *RUSSIAN AUTHORITIES UNVEIL UPDATED AI REGULATION FRAMEWORK*(2024), BRICS COMPETITION, https://www.bricscompetition.org/news/russian-authorities-unveil-updated-ai-regulation-framework#:~:text=Russia's%20updated%20artificial%20intelligence%20(AI,rather%20than%20foster%20their%20development
- 360 Business Law, *China's Approach to AI Regulation* (2025), 360 BUSINESS LAW, https://www.360businesslaw.com/blog/chinas-approach-to-ai-regulation/#:~:text=China's%20regulatory%20approach%20to%20AI%20demonstrates%20a%20dual%20strategy%3A%20promoting,ensure%20alignment%20with%20national%20interests
- Baiyand Xiao, *Agile and Iterative Governance: China's Regulatory Response to Ai* (2024), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4705898
- Wayne Wei Wang, *Artificial Intelligence "Law(s)" in China: Retrospect and Prospect* (2025), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5039316 .
- Jinghan Zeng, *Artificial and China's authoritarian governance* (2020), RESEARCHGATE, https://www.researchgate.net/publication/344678370_Artificial_intelligence_and_China's_authoritarian_governance
- State Council of China, *Next Generation Artificial Intelligence Development Plan* (2017), CHINA AEROSPACE STUDIES INSTITUTE, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-03-02%20China%27s%20New%20Generation%20Artificial%20Intelligence%20Development%20Plan-%202017.pdf

- National Governance Committee for the New Generation Artificial Intelligence, *Governance Principles for the New Generation Artificial Intelligence--Developing Responsible Artificial Intelligence* (2019), ChinaDaily, *https://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html*
- Cyberspace Admin. of China, *Internet Information Service Algorithmic Recommendation Management Provisions* (2022), https://www.cac.gov.cn/2021-12/31/c_1642894602930410.html
- Provisions on the Administration of Deep Synthesis of Internet Information Services (深度合成管理规定), China Law Translate, https://www.chinalawtranslate.com/en/deep-synthesis/ .
- *Interim Measures for the Management of Generative Artificial Intelligence Services* (2023) China Law Translate, https://www.chinalawtranslate.com/en/generative-ai-interim/
- China Briefing, *Ethical Review of Science and Technology in China: Draft Trial Measures* (2023), https://www.china-briefing.com/news/china-ethical-review-of-science-and-technology-draft-trial-measures/ .
- Shanghai New Generation AI Algorithm Innovation Action Plan (2021–2023), Shanghai Municipal People's Government, 2021.
- *Regulations of Shanghai Municipality on Promoting the Development of the Artificial Intelligence Sector*, 2022.
- *Regulations of Shenzhen Special Economic Zone on Promoting the Artificial Intelligence Industry*, 2022.
- *Zhonghua Renmin Gongheguo Minfa Dian* (中华人民共和国民法典) [Civil Code of the People's Republic of China], art. 1 (promulgated by the Standing Comm. Nat'l People's Cong., 2021).
- *Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa* (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China], art. 1 (adopted by the Standing Comm. Nat'l People's Cong., 2021).
- *Zhonghua Renmin Gongheguo Shuju Anquan Fa* (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China], art. 1 (adopted by the Standing Comm. Nat'l People's Cong., 2021).
- *Zhonghua Renmin Gongheguo Wangluo Anquan Fa* (中华人民共和国网络安全法) [Cybersecurity Law of the People's Republic of China], art. 1 (adopted by the Standing Comm. Nat'l People's Cong., 2017).
- *Zhonghua Renmin Gongheguo Dianzi Shangwu Fa* (中华人民共和国电子商务法) [E-Commerce Law of the People's Republic of China], art. 1 (adopted by the Standing Comm. Nat'l People's Cong., 2019).
- *Zhonghua Renmin Gongheguo Zhuzuoquan Fa* (中华人民共和国著作权法) [Copyright Law of the People's Republic of China], art. 1 (adopted by the Standing Comm. Nat'l People's Cong., 1991).
- *Guojia Guifan 个人信息安全规范* [Guidelines for Personal Information Security Specification], GB/T 35273-2020 (issued by Standardization Administration of China, 2020).
- China Translate, *Measures for Labeling of AI-Generated Synthetic Content* (2025), https://www.chinalawtranslate.com/en/ai-labeling/ .

- *Guójiā Guīfàn 个人信息安全规范* [Guidelines for Personal Information Security Specification], GB/T 35273-2020 (issued by Standardization Administration of China, 2020).
- *Xìnxī Ānquán Jìshù Jīqì Xuéxí Suànfǎ Ānquán Pínggū Guīfàn* (信息安全技术 机器学习算法安全评估规范) [Information Security Technology – Security Specification and Assessment Methods for Machine Learning Algorithms], GB/T 42888-2023 (issued by State Administration for Market Regulation & National Standardization Administration2024).
- *Xìnxī Ānquán Jìshù Gèrén Xìnxī Ānquán Yǐngxiǎng Pínggū Zhǐnán* (信息安全技术 个人信息安全影响评估指南) [Information Security Technology – Guidance for Personal Information Security Impact Assessment], GB/T 39335-2020 (issued by State Administration for Market Regulation & National Standardization Administration, 2021).
- White & Case, *AI Watch: Global regulatory tracker – China* (2025), WHITE & CASE, https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china
- State Council of the People's Republic of China, *New Generation Artificial Intelligence Development Plan*, State Council Document No.35 (2017).
- Ministry of Foreign Affairs, *Position Paper of the People's Republic of China on Regulating Military Applications of Artificial Intelligence (AI)* (2021), MINISTRY OF FOREIGN AFFAIRS THE PEOPLE'S REPUBLIC OF CHINA, https://www.mfa.gov.cn/eng/zy/wjzc/202405/t20240531_11367523.html .
- Ministry of Foreign Affairs, *Position Paper of the People's Republic of China on Strengthening Ethical Governance of Artificial Intelligence (AI)* (2022), MINISTRY OF FOREIGN AFFAIRS THE PEOPLE'S REPUBLIC OF CHINA, ,https://www.fmprc.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/AI/202211/t20221117_10976730.html .
- *Guójiā Yǔnxǔ Xìnxī Ānquán Jìshù Xìtǒng Jìshù Guīfàn* (国家允许信息安全技术系统技术规范) [National Permitted Information Security Technology System Technical Specifications], GB/T 35273-2020 (issued by Standardization Administration of China, 2020).
- *Shēngchéng Shì Rén Gōng Zhìnéng Fúwù Guǎnlǐ Zànxíng Bànfǎ* (生成式人工智能服务管理暂行办法) [Interim Measures for the Administration of Generative Artificial Intelligence Services], issued by the Cyberspace Administration of China et al., 2023.
- *Zhōnghuá Rénmín Gònghéguó Kēxué Jìshù Jìnbù Fǎ* (中华人民共和国科学技术进步法) [Law of the People's Republic of China on Progress of Science and Technology], 2022.
- *Rén Gōng Zhìnéng Shēngchéng Nèiróng Biāo Zhì Bànfǎ* (人工智能生成内容标识办法) [Measures for Labeling Artificial Intelligence-Generated Content], issued by the Cyberspace Administration of China et al., 2025.
- Yan Luo & Huezi Dan, *China Releases New Labeling Requirements for AI- Generated Content* (2025), COVINGTON, https://www.insideprivacy.com/international/china/china-releases-new-labeling-requirements-for-ai-generated-content/.
- *Rén Gōng Zhìnéng Fǎ Shìfàn Fǎ 1.0 Zhuānjiā Jiànyì Gǎo* (人工智能法 示范法 1.0 专家建议稿) [Artificial Intelligence Law, Model Law v. 1.0 (Expert Suggestion Draft)], issued by the Chinese Academy of Social Sciences, 2023.

- *Wǎngluò Shùjù Ānquán Guǎnlǐ Tiáolì* (网络数据安全管理条例) [Regulations on the Administration of Network Data Security], issued by the State Council of the People's Republic of China, 2025.
- *Wèichéngniánrén Wǎngluò Bǎohù Tiáolì* (未成年人网络保护条例) [Regulations on the Protection of Minors on the Internet], issued by the State Council of the People's Republic of China, Order No. 766, 2024.
- Faisal Santiago et al., *A Comparative Analysis of Artificial Intelligence Regulatory Law in Asia, Europe, and America* (2024), SHS Web of Conferences, https://www.shs-conferences.org/articles/shsconf/abs/2024/24/shsconf_diges-grace2024_07006/shsconf_diges-grace2024_07006.html
- Maulen Alimkanov, *Comparative Analysis of International AI Regulatory Approaches: The United States, European Union, Canada, China, Kazakhstan, Russia* (2024), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4873053 .
- Consolidated Version of the Treaty on European Union 2012 O.J. (C 326/13) 1.
- Tortoise – Global Ai, *The Global AI Index*, Tortoise Media, https://www.tortoisemedia.com/data/global-ai
- Justin Sherman, *Russia's digital tech isolationism: Domestic innovation, digital fragmentation, and the Kremlin's push to replace Western digital technology* (2024), Atlantic Council, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-digital-tech-isolationism/ .
- *See* Jon Chun et al., *Comparative Global AI Regulation: Policy Perspectives from the EU, China, and the US* (2024), ARXIV – Cornell University, https://arxiv.org/abs/2410.21279 .
- *Republic Act No. 10173*, An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes, § 1, 2012.
- S.B. 2047, 2023-2024 Leg., Reg. Sess.(Cal. 2024).
- Elham Tabassi, *Artificial Intelligence Risk Management Framework* (2023), NIST, https://doi.org/10.6028/NIST.AI.100-1.
- Mattew Kirk et al., *Key Insights on President Trump's New AI Executive Order and Policy % Regulatory Implications* (2025), Squire Patton Boggs, https://www.squirepattonboggs.com/en/insights/publications/2025/02/key-insights-on-president-trumps-new-ai-executive-order-and-policy-regulatory-implications.
- Interim Measures for the Management of Generative AI Services, issued by the Cyberspace Administration of China et al., 2023.
- *Measures for the Management of Scientific Data* (科学数据管理办法), issued by the State Council of the People's Republic of China, 2018.
- Yannic Mahé, *Divergent Paths: Comparing AI Regulation in the US, EU, and China* (2024), LinkedIn, https://www.linkedin.com/pulse/divergent-paths-comparing-ai-regulation-us-eu-china-yannick-mahé-ztlre/ .
- Josh China and Liza Lin, Surveillance State, (1st ed. 2022)
- Filippo Lancieri et al., *AI Regulation: Competition, Arbitrage & Regulatory Capture* (2025), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5049259
- *Regulation (EU) 2016/679*, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.
- Adam Set Litwin et al., *A Forum on Workplace AI Regulation Around the World*, 77 ILR Rev. 14 (2024).

- Anu Bradford, Digital Empires: The Global Battle to Regulate Technology (1st ed. 2023).
- *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2024), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
- Nibedita Basu et al., *COMPARATIVE ANALYSIS OF LAWS IN AI*, 5 SDG Rev. 17,18 (2024).
- José-Miguel Bello, *A first step on the long road to global AI regulation* (2024), The interpreter, https://www.lowyinstitute.org/the-interpreter/first-step-long-road-global-ai-regulation .
- Future of Privacy Forum, *THE WORLD'S FIRST BINDING TREATY ON ARTIFICIAL INTELLIGENCE, HUMAN RIGHTS, DEMOCRACY, AND THE RULE OF LAW: REGULATION OF AI IN BROAD STROKES* (2024), Future of Privacy Forum, https://fpf.org/blog/the-worlds-first-binding-treaty-on-artificial-intelligence-human-rights-democracy-and-the-rule-of-law-regulation-of-ai-in-broad-strokes/
- Shaping Europe's digital future, *Commission welcomes G7 leaders' agreement on Guiding Principles and a Code of Conduct on Artificial Intelligence* (2023), Digital Strategy, https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-g7-leaders-agreement-guiding-principles-and-code-conduct-artificial
- Shu Li et al., *Liability Rules for AI-Related Harm: Law and Economics Lessons for a European Approach*, 2022 CUP 1.
- Richik Sarkar et al., *Mitigating Board and Corporate Fiduciary Risks of AI*, 2025 Risk Management Magazine 1.
- Kai Zenner, *An AI Liability Regulation would complete the EU's AI strategy* (2025), CEPS, https://www.ceps.eu/an-ai-liability-regulation-would-complete-the-eus-ai-strategy/
- Joseph R. Tiano Jr. et al., *The Duty of Supervision in the Age of Generative AI: Urgent Mandates for a Public Company's Board of Directors and Its Executive and Legal Team*, 2024 Bus. Law Today 1.
- Smith v. Van Gorkom, 488 A.2d 858 (Del. 1985).
- Cede & Co. v. Technicolor, Inc., 634 A.2d 345 (Del. 1994).
- In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).
- *Stone v. Ritter*, 911 A.2d 362 (Del. 2006).
- *See* Gregory A. Markel et al., *A Director's Duty of Oversight after Marchand in "Caremark" Case* (2022), Harvard Law School Forum on Corporate Governance, https://corpgov.law.harvard.edu/2022/01/23/a-directors-duty-of-oversight-after-marchand-in-caremark-case/
- Lexi Legal Law, *The Legal Future: Artificial Intelligence and Corporate Law* (2025), mondaq, https://www.mondaq.com/turkey/corporate-governance/1566104/the-legal-future-artificial-intelligence-and-corporate-law.
- Amy Antoniolli et al., *ESG Update: Corporate Directors May Be Obligated to Assess Political Risk*, 2025 Nat. L. Rev. 1.
- Marchand v. Barnhill, 212 A.3d 805 (Del. 2019).
- In re The Boeing Co. Derivative Litig., C.A. No. 2019-0907-MTZ, 2021 WL 4059934 (Del. Ch. 2021).
- Teamsters Local 443 Health Servs. & Ins. Plan v. Chou, C.A. No. 2019-0816-SG, 2020 WL 5028065 (Del. Ch. 2020).
- In re Clovis Oncology, Inc. Derivative Litig., C.A. No. 2017-0222-JRS, 2019 WL 5054136 (Del. Ch. Oct. 1, 2019).
- Constr. Indus. Laborers Pension Fund v. Bingle, C.A. No. 2021-0940-SG, 2022 WL 4102492 (Del. Ch. 2022).

- Edmond & Lily Safra, *Post #6: The Caremark Rule and Board Level AI Risk Management* (2024), Center for Ethics – Harvard University, https://www.ethics.harvard.edu/blog/post-6-caremark-rule-and-board-level-ai-risk-management%C2%A0 .
- In re McDonald's Corp. Stockholder Derivative Litig*.,* C.A. No. 2021-0324-JTL, 291 A.3d 652 (Del. Ch. 2023).
- *Clem v. Skinner*, C.A. No. 2021-0240-LWW, 2024 WL 1050900 (Del. Ch. 2024).
- Gail Weinstein et al., *2024 Caremark Developments: Has the Court's Approach Schifted?* (2024), Harvard Law School Forum on Corporate Governance, https://corpgov.law.harvard.edu/2024/05/20/2024-caremark-developments-has-the-courts-approach-shifted/ .
- Zhonghua Renmin Gongheguo Gongsi Fa [Company Law of the People's Republic of China], Standing Committee of the National People's Congress, Dec. 29, 1993, in Zhonghua Renmin Gongheguo Fagui Haibian [Official Decree of the PRC], No. 59, 1 (1993).
- RsA asia, *Fiduciary Duty in China's New Company Law* (2024), RsA asia, https://www.rsa-tax.com/single-post/fiduciary-duty-in-china-s-new-company-law.
- *AI and directors' duties*, 2023 CBLJ 1.
- Hao Xue , *Legal Regulation of Artificial Intelligence Directors under the Background of the Revision of China's New Company Law* (2024), Research Gate, https://www.researchgate.net/publication/382766555_Legal_Regulation_of_Artificial_Intelligence_Directors_under_the_Background_of_the_Revision_of_China's_New_Company_Law/fulltext/66abf611299c327096a3331d/Legal-Regulation-of-Artificial-Intelligence-Directors-under-the-Background-of-the-Revision-of-Chinas-New-Company-Law.pdf
- Postanovleniia palat Federal'nogo Sobraniia [resolution of the State Duma] 2024, Bill No. 512628-8.
- Data Guidance, *Russia: Duma passes bill on insuring civil liability from AI use* (2024), Data Guidance, https://www.dataguidance.com/news/russia-duma-passes-bill-insuring-civil-liability-ai .
- Ugolonyī Kodeks Rossiīskoī Federatsii [UK RF] [Criminal Code] (Russ.).
- *Development of AI regulations in Russia*, 2025 ABLJ 1.
- European Parliament, *Artificial Intelligence Liability Directive*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf
- Caitlin Andrews, *European Commission withdraws AI Liability Directive from consideration* (2025), iapp, https://iapp.org/news/a/european-commission-withdraws-ai-liability-directive-from-consideration .
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of October 19,2022, on a single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), [OJ L 277, 27.10.2022] .
- Two Birds, *Remedies and liabilities,* Two Birds, https://www.twobirds.com/-/media/pdfs/gdpr-pdfs/71--guide-to-the-gdpr--remedies-and-liabilities.pdf .
- Peter Church et al., *The EU Digital Services Act: A new era for online harms and intermediary liability* (2023), Linklaters, https://www.linklaters.com/it-it/insights/blogs/digilinks/2023/february/the-eu-digital-services-act---a-new-era-for-online-harms-and-intermediary-liability .
- Chintan Dave, *Understanding DAOs and its Legal Liabilities* (2023), LinkedIn, https://www.linkedin.com/pulse/understanding-daos-its-legal-liabilities-chintan-blockchain-trainer/ .

- Sergey Ostrovskiy, *DAO 3.0: Ultimate Legal Structuring for DAOs in 2025 and Beyond* (2025), AURUM, https://aurum.law/newsroom/DAO-3-0-ultimate-dao-legal-structuring-in-2025-and-beyond .
- Samuels v. Lido DAO, No. 23-cv-06492-VC, 2024 WL 6782733 (N.D. Cal. Nov. 18, 2024).
- DAO 3.0: *The Harmony Framework (2025),* DAOBOX, https://harmony.daobox.io/.
- DAOBox, *Harmony TL;DR* (2025), DAOBOX, https://harmony.daobox.io/harmony-tl-dr-a-5-min-read .
- Sergey Ostrovskiy, *DAO 3.0: The Harmony Framework* (2025), DAOBOX, https://harmony.daobox.io .
- Bruce Barcott, *AI Lawsuits Worth Watching: A Curated Guide*, 2024 Tech Policy Press 1.
- Dan Milmo, *'Impossible' to create AI tools like ChatGPT without copyrighted material, OpenAI says* (2024), THE GUARDIAN, https://www.theguardian.com/technology/2024/jan/08/ai-tools-chatgpt-copyrighted-material-openai .
- Amy Wong et al., *Recent trends in Generative Artificial Intelligence Litigation in the United States* (2023), K&L GATES, https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023
- Dentons, *AI trends for 2025: Disputes and managing liability* (2025), DENTONS, https://www.dentons.com/en/insights/articles/2025/january/10/ai-trends-for-2025-disputes-and-managing-liability
- Thaler v. Vidal, 43 U.S. (Fed. Cir. 2022).
- Deidre M. Wells, *Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022) (Moore, Taranto, Stark)* (2023), STERNE KESSLER, https://www.sternekessler.com/news-insights/insights/thaler-v-vidal-43-f4th-1207-fed-cir-2022-moore-taranto-stark/.
- Monika J. Malek et al., *Thaler v. Vidal: Artificial Intelligence Inventions Create Real Issues* (2022), VEDDERPRICE, https://www.vedderprice.com/thaler-v-vidal-artificial-intelligence-inventions-create-real-issues
- Va. Code Ann. §§ 2.2-4000 to -4033 (2024).
- 35 U.S.C. (2023).
- Mohamad v. Palestinian Authority, 566 U.S. 449 (2012)
- Ji Mao, *Revisiting AI Inventorship in Thaler v. Vidal* (2022), HOLAND & KNIGHT, https://www.hklaw.com/en/insights/publications/2022/10/revisiting-ai-inteventorship-in-thaler-v-vidal
- *See* Akin, *Supreme Court Will Not Review United States Court of Appeals for the Federal Circuit's Decision in Thaler v. Vidal* (2023), AKIN GUMP, https://www.akingump.com/en/insights/ai-law-and-regulation-tracker/supreme-court-will-not-review-united-states-court-of-appeals-for-the-federal-circuits-decision-in-thaler-v-vidal
- The Authors Guild v. OpenAI Inc. et al. , No. 1:23-cv-08292 (2023).
- Michalsons, *Authors Guild et al. v OpenAI | Copyright Infringement*, MICHALSONS, https://www.michalsons.com/blog/authors-guild-v-openai-copyright-infringement/74945
- *See* Cornell Law School, *17 U.S. Code § 106 – Exclusive rights in copyrighted works,* https://www.law.cornell.edu/uscode/text/17/106#:~:text=The%20five%20fundamental%20rights%20that,stated%20generally%20in%20section%20106
- George R.R. Martin, *A Clash of Kings* (1998).
- The New York Times Co. v. Microsoft Corp. Et al.*,* No. 1:23-cv-11195, 2024 WL 4102492 (S.D.N.Y. 2024).
- 17 U.S.C. §§ 101–810 (2024).
- The Authors Guild, Inc. v. HathiTrust*,* 755 F.3d 87 (2d Cir. 2014).
- The Authors Guild, Inc. v. Google, Inc., 804 F.3d 202 (2d Cir. 2015).
- *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).

- *See State v. Loomis*, 130 Harv. L. Rev. 1 (2017).
- *See* Studicata, *State v. Loomis* (2016), STUDICATA, https://studicata.com/case-briefs/case/state-v-loomis/.
- MillerKing, LLC v. DoNotPay, Inc., No. 3:23-CV-863-NJR, 2023 WL 702244059 (S.D. Ill. 2023).
- 15 U.S.C. §§ 1051 et seq.
- Justia, *Illinois Law*, https://law.justia.com/illinois/
- Bod Ambrogi, *In Case of 'Real Lawyers Against A Robot Lawyer', Federal Court Dismisses Law Firm's Suit Against DoNotPay for Unauthorized Law Practice* (2023), LAWSITES, https://www.lawnext.com/2023/11/in-case-of-real-lawyers-against-a-robot-lawyer-federal-court-dismisses-law-firms-suit-against-donotpay-for-unauthorized-law-practice.html
- Faradian v. DoNotPay, 123 F.4th 456 (9th Cir. 2023).
- Lee v. DoNotPay, 123 F.4th 456 (9th Cir. 2023).
- Federal Trade Commission, *FTC Finalizes Order with DoNotPay that Prohibits Deceptive 'AI Lawyer' Claims, Imposes Monetary relief, and Requires Notice to Past Subscribers*(2025), FTC, https://www.ftc.gov/news-events/news/press-releases/2025/02/ftc-finalizes-order-donotpay-prohibits-deceptive-ai-lawyer-claims-imposes-monetary-relief-requires
- Garcia v. Character Technologies, Inc., No. 6:24-cv-01903, 2024 WL [pinpoint citation] (M.D. Fla. 2024).
- Social Media Victims Law Center, *Character.AI Lawsuits* (2025), SOCIAL MEDIA VICTIMS LAW CENTER https://socialmediavictims.org/character-ai-lawsuits/ .
- Kayne McGladrey, *Garcia v. Character.ai – Defendants File Motions to Compel Arbitration and Dismiss Claims* (2025), LINKEDIN, https://www.linkedin.com/pulse/garcia-v-characterai-defendants-file-motions-compel-kayne-mcgladrey-sdckc/ .
- 47 U.S.C. § 230 (2023).
- Legal Information Institute, *estoppel in pais*, https://www.law.cornell.edu/wex/estoppel_in_pais .
- Mobley v. Workday, Inc., No. 3:23-cv-00770-RFL, 2024 U.S. Dist. LEXIS 126336 (N.D. Cal. 2024).
- Civil Rights Division, *Federal Protections Against National Origin Discrimination* (2000), US DEPARTMENT OF JUSTICE, https://www.justice.gov/crt/federal-protections-against-national-origin-discrimination-1 .
- Annette Tyman, *Mobley v. Workay: Court Holds AI Service Providers Could Be Directly Liable for Employment* (2024), SETFARTH, https://www.seyfarth.com/news-insights/mobley-v-workday-court-holds-ai-service-providers-could-be-directly-liable-for-employment-discrimination-under-agent-theory.html .
- HRWorks, *Implications of Mobley v. Workday* (2024), HRWORKS, https://hrworks-inc.com/industry-update/implications-of-mobley-v-workday/#:~:text=Between%202017%20and%202024%2C%20Mobley,resulting%20in%20a%20disparate%20impact
- Civil Rights Act of 1964, Title VII, 42 U.S.C. § 2000e et seq. (2023).
- Katie Kerpel, *What Is Agency Theory?* (2024), INVESTOPEDIA, https://www.investopedia.com/terms/a/agencytheory.asp .
- Shari Davidson, *The Growth of AI Law: Exploring Legal Challenges in Artificial Intelligence*, 15 Nat. L. Rev. 1 (2025).
- Thaler v. Vidal, 43 (Fed. Cir. 2022).
- U.S. Copyright Office, Compendium of U.S. Copyright Office Practices § 101 (3d ed. 2021).

- World Lawyers Forum, *The Future of AI in Legal Practices: Opportunities & Challenges* (2025), WORLD LAWYERS FORUM, https://worldlawyersforum.org/articles/future-ai-legal-practice-opportunities-challenges/
- *See* American Bar Association, *ABA issues first ethics guidance on a lawyer's use of AI tools* (2024), ABA, https://www.americanbar.org/news/abanews/aba-news-archives/2024/07/aba-issues-first-ethics-guidance-ai-tools/ .
- Shodh Sagar, *Artificial Intelligence and the Future of Legal Practice: Opportunities and Ethical Challenges*, 2 Indian JL 1 (2024).
- Jaime Sevilla et al., *Can AI Scaling Continue Through 2030?* (2024), EPOCH AI, https://epoch.ai/blog/can-ai-scaling-continue-through-2030 .
- Casimir Rajnerowicz, *AI in Due Diligence: What It Means for M&A and Beyond* (2024), V7, https://www.v7labs.com/blog/ai-due-diligence .
- Thomson Reuters, *How Generative AI is Shaping the Future of Law: Challenges and Trends in the Legal Profession* (2025), THOMSON REUTERS, https://www.thomsonreuters.com/en-us/posts/innovation/how-generative-ai-is-shaping-the-future-of-law-challenges-and-trends-in-the-legal-profession/ .
- Shodh Sagar, *Artificial Intelligence and the Future of Legal Practice: Opportunities and Ethical Challenges*, 2 Indian JL 3 (2024).
- Bernice Melvin, *The future of Artificial Intelligence and legal careers* (2024), SMART LAWYER, https://nationaljurist.com/smartlawyer/the-future-of-artificial-intelligence-and-legal-careers/
- NexLaw.AI, *Navigating the Future of AI and Law*, https://www.nexlaw.ai/the-future-of-ai-and-law/ .
- DataGuidance, *Russia: Current status and development of AI regulations* (2024), DATA GUIDANCE, https://www.dataguidance.com/opinion/russia-current-status-and-development-ai .
- Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act, Pub. L. No. 119-12, 139 Stat. 102 (2025).
- Andrew r. Chow, *Inside the First Major U.S. Bill Tackling AI Harms – and Deepfake Abuse*, 2025 Time 1.
- Garcia v. Character Technologies*, Inc.*, No. 6:24-cv-01903-ACC-UAM, 2025 WL 1461721 (M.D. Fla. 2025).
- The Authors Guild v. OpenAI Inc.*,* No. 1:23-cv-08292 (S.D.N.Y. 2023).
- Michalsons, *Authors Guild v OpenAI | Copyright Infringement*, https://www.michalsons.com/blog/authors-guild-v-openai-copyright-infringement/74945.
- *Charting a course with AI* regulation, 2025 IBLJ 1 .
- Sandra Watcher, *Limitation and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*, 26 YJoLT 5 (2024).