SÖDERTÖRNS UNIVERSITY

MASTER'S DISSERTATION

A Rights-Based Approach to Artificial Intelligence

— An Analysis of Regulatory Measures in the European Union, the United States, and China

Author:
Sinead Cassandra Sammy

Supervisor:
Monirul Azam

A dissertation submitted in fulfilment of the requirements

for the degree of Masters in Public Law

in the Department of Social Sciences

January 2026

SÖDERTÖRNS UNIVERSITY

Abstract

Department of Social Sciences

Masters of Public Law

A Rights-Based Approach to Artificial Intelligence
— An Analysis of Regulatory Measures in the European Union, the United States, and China

by Sinead Cassandra Sammy

This study adopts a rights-focused perspective to evaluate how Artificial Intelligence (AI) is regulated in the European Union, the United States, and China through a legal analysis. It uses a three-jurisdiction framework to examine the EU AI Act, assess its implications for fundamental rights and contrast it with AI regulatory approaches in the United States and China. The analysis focuses on how these legal frameworks safeguard fundamental rights and structure accountability in the development and deployment of AI systems. Drawing on doctrinal analysis of existing regulations, legal documents, case law and academic literature, the study identifies significant differences in regulatory strategies—ranging from rights-based and risk-based models to more security driven and market driven approaches. It concludes with recommendations for regulatory convergence and policy harmonisation aimed at strengthening human rights protection, transparency and accountability in AI governance.

Keywords: Artificial Intelligence; Regulation and Legislation of AI; AI systems; EU law; Fundamental rights; Human rights law; Privacy and Data protection; Non-Discrimination; Expression; Fairness and Explanation; Ethical AI governance; Accountability and Transparency; Sustainable Development Goals; Legal dogmatic method; European Union; United States; China.

Acknowledgements

I wish to express my sincere gratitude to my supervisor, ***Monirul Azam***, for his invaluable support and guidance throughout the development of this dissertation. His insights have been crucial in examining this relevant and evolving subject, particularly in shaping the analysis of how AI systems may threaten or impact fundamental rights and in refining the translation and interpretation of the relevant regulations.

This dissertation provides direct translations of certain regulations and highlights four key fundamental rights, illustrating how they might be at risk or have already been affected by AI systems. It also details the guidelines that developers, deployers and users of AI technologies should follow when creating or using these technologies.

Stockholm, 2026

Contents

Abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
CCPA	California Consumer Privacy Act (US)
CJEU	Court of Justice of the European Union (EU)
CPRA	California Privacy Rights Act (US)
ECHR	European Convention on Human Rights (EU)
EU	European Union
EU AI Act	European Unions Artificial Intelligence Act (EU)
FRIA	Fundamental Rights Impact Assessment
GDPR	General Data Protection Regulation (EU)
HR	Human Rights
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic, Social and Cultural Rights
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PIPL	Personal Information Protection Law (China)
TFEU	Treaty on the Functioning of the European Union (EU)
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organisation
US	United States

Glossary

Term	Definition
Algorithmic	Expanding digital.
Algorithmic Accountability & Responsibility	Obligations and responsibilities for AI developers, deployers and designers to make sure that their AI systems act accountable and follow the laws. The AI systems must operate legally, fairly, ethically and transparently with machines that detect or correct errors and biases.
Algorithmic Bias & Discrimination	Repetitive errors in an AI system's decision-making which may have resulted in some form of discrimination, bias or unfairness against someone or a group of people.
Algorithmic Sustainability	Expanding digital and AI technologies in a way that stabilises economic, social and environmental sustainability while reducing harm.
Algorithmic Transparency	AI systems that stakeholders and users can understand, trust and hold responsible.
Artificial Intelligence	Technological machines that have the capability to imitate human-like intellectual functions like reasoning, learning and making decisions through computer simulation.
Deep Learning	A sophisticated form of machine learning that uses foundation models to unfold data patterns.
Digital Sovereignty	A state's or region's capability to keep control over its digital infrastructure, data and information systems.
Ethical AI	AI systems that conform to ethical standards by upholding fairness, transparency, accountability, respect for human rights and a person's well-being.

Term	Definition
Hard Laws	Regulations, statutes, treaties and court decisions which are legally binding and put a responsibility on states and countries to implement them into national regulation.
Human-Robot Interaction	A multidisciplinary study on the interaction between robots and humans. This involves the design, usage, development, ethics, deployment of AI systems and the societal impacts that robots may have on the people.
Machine Learning	A branch of AI systems that enables computer algorithms to improve their performance through obtaining and learning information from data without direct programming.
Regulatory Framework	A set of regulations, policies and guidelines put in place by a country's or a state's government in order to ensure compliance when it comes to the protection of the people's rights, businesses and the country's or states territory.
Soft Laws	Principles, agreements, guidelines, declarations or recommendations that are non-binding. States can choose whether to implement them into national regulation or not.

Chapter 1

Introduction

Artificial intelligence (AI) has become a crucial component of contemporary society, revolutionising industries and influencing decision-making processes. AI systems are applied to automate tasks, improve efficiency and manage substantial volumes of data in fields such as healthcare, finance, law enforcement, education and public governance.[1] Yet, as AI progresses, there are rising concerns about its effects on fundamental rights,[2] especially regarding privacy, data protection and non-discrimination.[3]

One of the most urgent concerns is the degree to which AI systems gather, analyse and operate using personal data, often without individuals' complete awareness or consent.[4] Automated recruitment systems, biometric monitoring, predictive policing and credit scoring algorithms illustrate how AI can impact key life choices, sometimes perpetuating biases, reducing transparency or compromising due process.[5] These challenges underscore the need for legal protections to ensure that AI complies with human rights standards.

The regulation of AI has become a primary focus for global policymakers. The European Union (EU), the United States (US) and China have each developed different approaches to AI governance, influenced by their respective legal traditions and policy objectives.[6] The EU has implemented a risk-based regulatory structure through the EU AI Act, while the US predominantly uses sector-specific guidelines and voluntary frameworks. China adopts a more centralised, state-directed model. Nevertheless, these

[1] *See*, Pekka Salokannel, "The Impact of AI: How Artificial Intelligence is Transforming Society", *3DBear Blog* (2023), available at www.3dbear.io/blog, accessed on 1 May 2025.

[2] *See*, Amnesty International, "The Urgent but Difficult Task of Regulating Artificial Intelligence" (2024), available at amnesty.org/ai-regulation, accessed on 28 April 2025; *See also*, Rowena Rodrigues, "Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities", *Journal of Responsible Technology* (2020), Vol. 4, available at doi:10.1016/j.jrt.2020.100005, accessed on 26 May 2025.

[3] Rodrigues, *supra* note 2; *See*, Office of the Victorian Information Commissioner, "Artificial Intelligence and Privacy – Issues and Challenges" (2021), available at ovic.vic.gov.au/ai-privacy, accessed on 3 June 2025.

[4] *See*, DataGuard Insights, "The Growing Data Privacy Concerns with AI: What You Need to Know" (2024), available at dataguard.com/ai-privacy, accessed on 3 June 2025.

[5] Rodrigues, *supra* note 2.

[6] *See*, Emmanuel Pernot-Leplay, "The AI Dilemma: AI Regulation in China, EU & the U.S." (2025), available at pernot-leplay.com/ai-dilemma, accessed on 24 July 2025.

approaches still exhibit shortcomings in ensuring accountability, transparency and the safeguarding of fundamental rights.[7]

In light of these regulatory differences, it is crucial to adopt a rights-based approach to AI governance to ensure that technological progress does not undermine fundamental rights. While current legal frameworks strive to balance innovation with necessary protections, doubts persist about their capacity to effectively tackle issues such as discrimination, opacity and excessive surveillance.[8] This research evaluates how effectively these frameworks safeguard fundamental rights and identifies lessons to be incorporated to improve global AI governance through a legal analysis of AI regulations in the EU, the US, and China.

1.1 Research Issue and Main Questions

This research aims to examine the legal and regulatory systems governing AI in the EU, the US, and China, emphasising a rights-based perspective. By comparing the regulatory frameworks and legal protections in these regions, the study evaluates the effectiveness of current laws in defending fundamental rights. It explores the Obstacles involved in aligning AI governance with international human rights norms. Additionally, the research aims to identify exemplary practices that can support the development of reliable and sustainable AI governance on both regional and global scales. The study is driven by the following questions:

(i) How do the EU, the US, and China address fundamental rights in their AI regulations?

(ii) What balances and obstacles exist to ensure rights-based AI regulations?

1.2 Research Method and Legal Perspective

This dissertation employs the *Legal dogmatic* method to examine the regulatory framework and address the research questions. This method focuses on *de lege lata*, analysing current laws in the EU, the US, and China pertaining to AI regulation and its effects on fundamental rights.[9] Using a legal-dogmatic approach, the dissertation offers a systematic interpretation and comparison of relevant hard and soft law across the examined jurisdictions. It places particular emphasis on legal instruments that directly or indirectly govern the design, deployment, and oversight of AI systems.

[7] Rodrigues, *supra* note 2.

[8] Ibid.

[9] *See*, Aleksander Peczenik, "Empirical Foundations of Legal Dogmatics", *Logique et Analyse, Nouvelle Série* , Vol. 12: Iss. 45 (1969): p. 32, available at jstor.org/peczenik, accessed on 20 April 2025.

1.3 Research Significance and Contributions

This study adds to the ongoing dialogue on AI regulation by examining the structures of existing legal frameworks in the EU, the US, and China. It questions whether these laws should be modified to better safeguard fundamental rights and promote sustainability. The significance of this research is highlighted by its emphasis on the rapidly evolving field of AI systems and the increasing demand for more defined rights-based regulations that uphold human dignity and promote the ethical application of AI technology.

1.4 Research Dissertation Structure

The dissertation consists of five chapters:

Chapter 1: Introduction — outlines the research problem and questions, the methodology and the broader significance of the dissertation.

Chapter 2: AI Regulatory Framework — provides an overview of AI regulation in the EU, the US, and China.

Chapter 3: Fundamental Rights Approach — examines how fundamental rights are integrated into AI regulatory frameworks across these jurisdictions, with a focus on four key human rights central to the topic.

Chapter 4: Balances and Obstacles — explores the tensions, trade-offs and practical challenges involved in regulating AI so as to safeguard individual rights while promoting innovation.

Chapter 5: Conclusion and Policy Recommendations — synthesises the main findings and proposes policy recommendations for rights-based AI regulation in the three jurisdictions.

Chapter 2

AI Regulatory Framework

The rapid development of AI has greatly influenced both private and public domains, prompting transformations in numerous fields such as healthcare, decision-making, digital products, applications and media. As AI becomes more embedded in everyday life and takes a prominent role, it prompts discussions on its reliability, accountability and the need for regulatory oversight.[10] This chapter presents the regulatory structures that manage AI on an international scale, as well as within the EU, the US, and China.

2.1 A Brief Overview of Global AI Regulation

Globally, there is still an absence of binding regulations for AI that guarantees its development and use adhere to human rights and public law principles. Instead of strict rules, there are only non-binding recommendations provided by intergovernmental organisations. These guidelines outline essential principles that AI developers should follow to maintain democratic and ethical standards. An important primary international guidelines framework is the AI Principles set by the Organisation for Economic Co-operation and Development.

2.1.1 OECD Legal Instruments Recommendation of the Council on Artificial Intelligence

In 2019, the Organisation for Economic Co-operation and Development (OECD) introduced a Council Recommendation concerning AI.[11] This soft law regulatory framework sets forth standards and guidelines for OECD member countries to follow, with the aim of fostering innovative and reliable AI systems globally.[12] The framework's principles provide a thorough approach to ensure that AI systems are developed and implemented in a way that promotes trustworthiness. Furthermore, these principles are

[10] *See*, Monirul Azam, "Artificial Intelligence and EU Law: Risk, Sustainability and Public Good", in *AI and Fundamental Rights under the EU Law*, edited by Claes, Katarina & Christina (2019): p. 85.

[11] *See*, UNESCO, "Recommendation on the Ethics of Artificial Intelligence" (2021), available at unesco.org/ai-ethics, accessed on 3 April 2025.

[12] *See*, OECD, "OECD AI Principles overview" (2019), available at oecd.ai/principles, accessed on 30 March 2025.

supported by five concrete recommendations for policymakers aimed at guiding AI development according to Public Law Values and the Sustainable Development Goals[13].[14]

Five Guidelines for the Responsible Management of AI

The *first principle* acknowledges that the aim of creating and applying reliable AI systems is to prioritise sustainable development and the well-being of individuals and the planet. The key objectives of AI systems include promoting creativity, increasing productivity and helping to conserve the environment. AI should be accessible to everyone to help mitigate current social, economic and gender biases, along with other global inequalities. This principle is in harmony with various international human rights frameworks and seeks to build public trust through their understanding of AI.[15]

The *second principle* emphasises that AI developers must ensure that AI systems adhere to the rule of law, democratic values and human rights throughout their entire lifecycle. This encompasses safeguarding individual rights to fairness, non-discrimination, privacy and access to justice. AI developers are required to implement strong security measures to protect against potential, intentional or unintentional misuse of AI technology.[16]

The *third principle* stresses the necessity for transparent AI systems that provide clear documentation of both their capabilities and limitations. AI developers should ensure that their systems can offer information and explanations to people adversely affected by AI decisions, allowing them the opportunity to contest the outcomes driven by AI.[17]

The *fourth principle* requires that AI systems be robust, safe and secure throughout their lifetime. The AI systems should operate correctly, withstand cyberattacks and errors and be able to be repaired in order to prevent harm or unwanted behaviour. Developers should incorporate additional mechanisms to enhance information integrity and protect freedom of expression. These actions ensure that AI systems remain safe, trustworthy and minimise potential risks.[18]

The *final principle* highlights the accountability that AI developers must assume for the operation of their AI systems and they should be responsible for the decisions these systems make. Developers must comply with the aforementioned principles and ensure the traceability of AI decisions by implementing effective risk management processes. This approach is essential

[13] The Sustainable Development Goals include 17 worldwide objectives that are intended to be accomplished by 2030. These goals require prompt actions to improve and protect the peace and well-being of both our planet and those who live on it, currently and in the future. *See*, United Nations, "The 17 Sustainable Development Goals" (2015), available at un.org/sustainable-development-goals, accessed on 3 December 2025.

[14] OECD, *supra* note 12.

[15] OECD AI Principle 1.1.

[16] OECD AI Principle 1.2.

[17] OECD AI Principle 1.3.

[18] OECD AI Principle 1.4.

to developing trustworthy AI systems that reduce the harm and adverse effects associated with AI usage.[19]

2.2 AI Regulation in the EU

The EU has positioned itself as a leader in AI regulation, focusing on human rights, fairness and transparency. Its AI regulatory strategy is based on a risk-based framework, categorising AI applications by their potential risk to individuals and society. This structure guarantees that AI applications with higher risks face more rigorous regulations, whereas lower-risk systems are granted more flexibility. The EU's AI Act represents significant legislation designed to ensure the secure and reliable application of AI technologies throughout the Union.

2.2.1 The EU Artificial Intelligence Act

In 2021, the EU Commission introduced an AI regulation known as the EU AI Act (Regulation (EU) 2024/1689)[20], which became effective in August 2024. The regulation's various parts have staggered implementation dates. Each EU member state is given two to three years to fully implement them and must designate three types of authorities that are responsible for ensuring compliance with the AI regulation.[21] This regulation as the world's first-ever regulation on AI, the EU AI Act establishes a significant legal framework to ensure AI technologies adhere to individual rights protection, uphold EU values, promote transparency and fairness.[22]

The primary aim of the EU AI Act is to establish a risk-oriented framework that enforces legal standards to reduce the potential risks posed by AI systems to individuals and society. Essentially, it strives to ensure that the advancement of AI technologies aligns with EU safety standards and that AI systems are deployed in a manner that fosters trust. Both providers and deployments of AI systems are obligated to ensure that their AI technologies comply with this EU regulation.[23]

The EU AI Act emphasises the necessity of safeguarding individual's safety, health and fundamental rights concerning the usage of AI technology. It assigns a responsibility to AI investors and developers to consider these fundamental rights, particularly if their AI systems are intended for use within

[19] OECD AI Principle 1.5.

[20] *See*, European Union, *Artificial Intelligence Act* (2024), Article 113, available at eur-lex.europa.eu/ai-act, accessed on 9 November 2025.

[21] *See*, Consolidated version of the Treaty on European Union (TFEU), *OJ C 326/13* (2012), Articles 288 and 297, available at eur-lex.europa.eu/teu, accessed on 3 May 2025; *See also*, Future of Life Institute, "Overview of all AI Act National Implementation Plans" (2024), available at artificialintelligenceact.eu/implementation, accessed on 3 December 2025.

[22] *See*, European Parliament, "EU AI Act: first regulation on artificial intelligence" (2024), available at europarl.europa.eu/ai-act, accessed on 8 July 2025.

[23] Azam, *supra* note 10, p. 91–92.

the EU. Additionally, this regulation extends to various marketing providers that operate AI systems in the Union.[24]

The initial four articles in Chapter I of the EU AI Act, effective as of February 2025, outline the legal framework concerning AI usage, specifying the applicable parties and providing various definitions relevant to the regulation. The Act identifies areas where AI is banned, the necessary requirements for AI systems to safeguard human rights and instances where AI usage is permissible. Other sections of the AI regulation provide further clarification on what is allowed and what is not. Breaches of this regulation may result in fines and penalties of up to €35 million or 7% of its entire global yearly turnover from the previous financial year, depending on the specific Article that has been violated.[25]

The EU AI Act categorises AI systems into four risk levels: I. *Prohibited* AI systems, II. *High-risk* AI systems, III. *Limited-risk* AI systems and IV. *Minimal-risk* AI systems. The I. *Prohibited* AI systems and II. *High-risk* AI systems are highlighted in the EU AI Act due to the necessity for regulations aimed at enhancing the protection of individual rights.[26]

I. Prohibited AI systems

Chapter II, Article 5 of the EU AI Act, which took effect in February 2025, outlines specific prohibitions on certain AI systems within the EU.[27] These bans target AI systems that are intended to manipulate, deceive or exploit vulnerable populations, potentially leading individuals to make an adverse decision they would not have made without AI influence. Such manipulation that compromises a person's capacity to make independent and potentially risky decisions is forbidden. Harmful decisions are defined as those that can cause mental, physical or financial harm to an individual or another person's well-being. For example, an AI system might fool someone into investing money, resulting in financial loss and poverty or manipulate individuals to inflict harm on religious minorities.[28]

AI systems that evaluate an individuals social behaviour to assign a social score are prohibited if this results in any form of discrimination against individuals or groups based on their social behaviour or personality traits. Specifically, AI systems cannot provide negative treatment to someone based on personality and behavioural data collected in a different context unrelated to the current situation.[29] Furthermore, AI risk assessment for predicting criminal offences is banned when someone's judgment is based on personality traits rather than their criminal conduct.[30]

[24] EU AI Act, Article 2.
[25] EU AI Act, Articles 99–101.
[26] European Parliament, *supra* note 22.
[27] EU AI Act, Article 113(a) and Recital 179.
[28] EU AI Act, Article 5(1)(a–b) and Recital 29.
[29] EU AI Act, Article 5(1)(c) and Recital 31.
[30] EU AI Act, Article 5(1)(d) and Recital 42.

The AI systems which are used to expand or develop facial recognition databases by incorporating facial images from Closed-Circuit Television (CCTV) footage or the Internet are prohibited, as they contribute to individuals feeling deprived of privacy and subject to mass surveillance.[31] AI systems designed to deduce or recognise people's expressions and emotions using their biometric data, particularly at work and in educational settings, are banned due to the potential for discriminatory consequences and breaches of fundamental rights. However, exceptions are allowed for purposes related to medical or safety concerns.[32]

Biometric AI systems that categorise individual's biometric data through fingerprints or facial recognition to infer or deduce race, political views, religious or philosophical beliefs, sex life, sexual orientation or trade union membership are partially prohibited. There are exceptions, especially in law enforcement, where biometric identification data is essential for analysing images to verify, locate and find missing persons, victims of assault or criminals. Furthermore, real-time remote biometric identification AI systems can be used in public spaces to identify individuals and prevent significant, imminent or terrorist threats.[33]

II. High-risk AI systems

Chapter III of the EU AI Act, titled High-risk AI systems, is structured into four sections and is set to be enforced starting on 2nd of August 2026, with certain exceptions. However, Section 4 of Chapter III has been in effect since August 2025, while Article 6(1) of the EU AI Act will take effect from August 2027.[34]

AI systems that are deemed high-risk are those that could potentially endanger an individuals safety, health or violate their fundamental rights.[35] Article 6(2–4), along with Annex III of the EU AI Act, outlines *eight specific AI systems* classified as high-risk but not banned, provided they undergo testing before market release and comply with the necessary standards for sale or use within the EU.[36]

The EU AI Act identifies the following categories of AI systems as *high-risk*:

The *first category* includes the AI biometric data systems used in biometric categorisation and verification, which fall under the personal data group. These systems must be labelled as high-risk due to the technological errors and risks that can arise in these AI systems through prejudice or discriminatory measures. For example, remote biometric identification where a person is treated unfairly due to their disability, race, sex, etc.[37]

[31] EU AI Act, Article 5(1)(e) and Recital 43.
[32] EU AI Act, Article 5(1)(f) and Recital 44.
[33] EU AI Act, Article 5(1)(g–h), Recitals 30, 32–33, 38–41 and Annex II.
[34] EU AI Act, Article 113(b–c) and Recital 178.
[35] EU AI Act, Article 6(2–4) and Recital 52.
[36] EU AI Act, Article 6(2), Article 50 and Annex III.
[37] EU AI Act, Annex III(1), Recitals 54 and 159.

AI systems intended for use as protective measures in the management and operation of essential digital infrastructure, road transportation and the supply of gas, water, electricity and heating is the *second category* that should be classified as high-risk. This classification is due to the potential negative impacts on individual life, safety, health and property if these AI systems malfunction. Consequently, AI developers have a greater responsibility to ensure that these systems are recognised as high-risk and are designed to incorporate safety measures. Warnings should be issued to help monitor risks and address cybersecurity concerns.[38]

AI systems used for educational and vocational training, which assess, evaluate, assign or analyse a person's behavioural and cognitive abilities, are the *third category* that must be deemed high-risk due to their potential to profoundly affect an individuals career or livelihood. It is crucial to ensure that these systems do not assess a person's abilities based on gender, race or sexuality, leading to discrimination.[39]

AI systems intended for use in various forms of employment and worker management are the *fourth* ones that should be categorised as high-risk due to their potential impact on worker's rights, livelihoods and future career prospects. Instances where such impacts or forms of discrimination could occur include recruitment, work-related decision-making, binding agreements, behaviour-based task assignments and judgments based on personal characteristics, traits or evaluations of an individual's contractual commitment. These AI systems must adhere to the protection of individual rights.[40]

The *fift*h scenario in which AI systems should also be classified as high-risk is when private or government entities employ AI to evaluate a person's lifestyle, insurance, financial status, creditworthiness or benefit eligibility. Such determinations can have a profound impact on a person's access to essential resources like urgent assistance, emergency services or safety. The deployment of AI in these contexts presents significant threats to personal rights and well-being, as mistakes or biased decisions could have serious consequences for those depending on these services.[41]

AI systems intended for use by law enforcement agencies that are neither thoroughly trained nor well-designed, documented, explainable, transparent and do not meet necessary standards or undergo testing before being introduced to the market are the *sixth category* that must be identified as high-risk. This is due to the potential power imbalance of AI systems, which could lead to issues such as surveillance, deprivation, unfairness, arrest or violations of an individuals fundamental rights and freedoms.[42]

The *seventh category* is those AI systems used in border control management, which should be regarded as high-risk applications due to their significant impact on vulnerable populations, such as asylum seekers and

[38] EU AI Act, Annex III(2) and Recital 55.
[39] EU AI Act, Annex III(3) and Recital 56.
[40] EU AI Act, Annex III(4) and Recital 57.
[41] EU AI Act, Annex III(5) and Recital 58.
[42] EU AI Act, Annex III(6) and Recital 59.

migrants. These systems present serious issues, such as potential bias, lack of transparency, inaccuracies and discriminatory practices. It is the responsibility of governments to ensure that these AI systems are thoroughly evaluated and tested prior to deployment to prevent the violation of fundamental rights. Furthermore, legal and ethical standards must be implemented to ensure that these systems respect individual rights and protections, thereby avoiding adverse social and humanitarian effects.[43]

Certain AI systems intended for use in democratic processes and the administration of justice are the *last* that should be classified as high-risk due to their potential effects on the rule of law, election voting, democracy and individual rights. It is crucial to address all forms of bias, lack of transparency and errors, especially when these AI systems are meant for be used within judicial and political authorities.[44]

2.3 AI Regulation in the US

The US is a key contributor to the advancement of AI technology, mainly focusing on non-regulatory strategies to foster development and innovation within its industries.[45] US government policies are structured to support AI advancement through approaches driven by standards for current AI technological progress.[46] At the federal level, the US lacks specific AI regulations but instead offers soft law ethical guidelines from the House of Representatives and the government. These guidelines aim to inform AI developers about essential considerations for ensuring that their AI respects human dignity, rights and transparency.

2.3.1 Blueprint for an AI Bill of Rights

The *Blueprint for an AI Bill of Rights* is a document released online in the US by President Biden's administration in 2022. Its primary objective is to create a framework based on rights to guide AI governance in the nation. Although not legally enforceable, it serves as a legal recommendation that presents five key principles aimed at safeguarding individual rights against harmful AI practices. The AI Bill of Rights highlights risks such as safety, human alternatives, data privacy, algorithmic bias or discrimination, and the right of individuals to receive explanations for AI-driven decisions. It emphasises that AI developers should ensure that their systems respect human dignity,

[43] EU AI Act, Annex III(7) and Recital 60.

[44] EU AI Act, Annex III(8) and Recitals 61–62.

[45] *See*, Xinbo Huang et al., "The Legal Challenges and Regulatory Responses to Artificial Intelligence (AI) in China", in *Proceedings of the 12th UUM International Legal Conference 2023* (2024): p. 336, available at doi.org/10.2991/ai-china, accessed on 9 September 2025.

[46] *See*, Yoon Chae, "U.S. AI Regulation Guide: Legislative Overview and Practical Considerations", in *RAIL: The Journal of Robotics, Artificial Intelligence & Law*, Vol. 3: Iss. 1 (2020): pp. 19–20.

maintain transparency and allow people to challenge AI systems if their rights are violated.[47]

Five core principles and their related practices in the Blueprint for an AI Bill of Rights

The *first principle* emphasises the need to protect people from ineffective and unsafe automated AI systems. Independent experts recommend that the creation of these systems be examined, evaluated and reported on to identify potential effects, risks and concerns for stakeholders and various communities. Safety measures, effectiveness and results should be examined through testing, monitoring, identification, risk assessment and mitigation before these systems are deployed or reasons for their removal are determined. Automated AI systems should not be designed if they pose a threat to individual or community safety. There should be protection against the misuse of irrelevant and inappropriate data during the development, design and deployment of AI systems. This is particularly important for automated AI systems that might cause significant damage through their reuse. Whenever possible, the findings of these investigations should be made publicly available.[48]

The *second principle* is concerned with protecting individuals from algorithmic discrimination, ensuring that AI systems and algorithms do not subject anyone to discrimination. AI systems must not promote unfair treatment by discriminating against individuals based on factors such as race, colour, sex, ethnicity, age, religion, national origin, disability, veteran status, genetic information or any legally prohibited grounds. The responsibility lies with AI deployers and developers to ensure that their systems do not infringe upon individual rights. These AI systems should operate fairly. Incorporating Proactive Equity Assessments into AI system designs is essential to shield data from serving as a proxy for demographic characteristics. Accessibility for people with disabilities must be ensured so that they can understand and interact with AI systems. To verify compliance with individual rights protections, independent evaluations and reports should be conducted to assess and identify the outcomes of AI systems.[49]

Principle three emphasises the importance of protecting individuals from privacy breaches by offering them design options that clarify what they consent to and what data will be collected. AI developers, designers and employers are required to obtain an individuals permission and honour any decision made regarding the collection, access, use, deletion and transfer of their data. This process should be conducted in a manner that respects a person's privacy rights and aligns with the individuals consent concerning which data may or may not be collected. Clear, concise and easily understandable language should be used to facilitate consent for data use. In situations where data fall into sensitive categories, such as

[47] *See*, White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights* (2022), available at whitehouse.gov/ai-bill-of-rights, accessed on 3 March 2025.

[48] AI Bill of Rights, Safe and Effective Systems.

[49] AI Bill of Rights, Algorithmic Discrimination Protections.

healthcare, employment, finance, education and criminal records, data can only be used if essential and must be protected from ethical violations and prohibited usage scenarios. Individuals must be protected from unwarranted technological surveillance that could cause harm or threaten their civil liberties and privacy. Continuous surveillance and monitoring are not to be employed in workplaces, educational settings, housing or any other context where they could restrict access, opportunities or rights. If such situations arise, it is preferable for individuals to receive reports or documentation detailing what they have consented to regarding their personal data.[50]

The *fourth principle* emphasises that people should be informed when AI systems are employed, ensuring that they understand the purpose and functioning of these systems, as well as the potential outcomes of automated decisions. It is essential for AI developers, designers and deployers to provide clear, timely and easily accessible information. This information should detail the role of AI systems and the reasoning behind their use. Those affected by AI-driven decisions should be notified of any changes, with regular updates included. individuals have the right to know the basis for decisions made by AI and the resulting implications. Clear explanations of how these systems operate, how they are interpreted and the associated risks should be provided. Additionally, a comprehensive report about AI must be publicly available.[51]

Principle five emphasises that individuals should have the right to opt out of participating in automated AI systems, choosing instead to interact with a human. This is particularly important in situations where an AI system might cause harm to an individual. If there is an error, failure or if someone wants to challenge a decision made by an AI, they should have the right to have their case reviewed by a person. It is crucial to have human oversight and consideration to ensure that public compliance remains fair and balanced. Automated AI systems intended for use in sensitive areas such as criminal justice, education, employment and health should be specifically designed for their roles and should involve human participation in decisions that are high-risk or adverse. Additionally, public reporting should be available so that people can understand and verify how their rights are being respected in these scenarios.[52]

Artificial Intelligence Risk Management Framework

In 2023, the National Institute of Standards and Technology (NIST) released the NIST AI RMF 1.0, which establishes technical standard guidelines for the responsible deployment of AI. This framework provides practical tools and best practices to manage risks related to AI systems, such as data bias, transparency and fairness concerns. The NIST AI RMF guidelines are crucial for AI developers, offering a roadmap to ensure compliance with industry standards, address potential risks and implement voluntary risk mitigation strategies. Essentially, AI system developers focus on individual rights,

[50] AI Bill of Rights, Data Privacy.
[51] AI Bill of Rights, Notice and Explanation.
[52] AI Bill of Rights, Human Alternatives, Consideration and Fallback.

sustainability and responsibility, which ultimately enhances the credibility of AI technologies for individuals.[53]

2.3.2 State-Level AI Regulations in the US

Although there is no federal AI regulation in the US, this has not deterred several states from either implementing or proposing their own AI regulations to safeguard people and their rights against AI-related risks or biases.[54] Examples of some US States that have enacted AI regulations include California, Oregon, Texas, Arizona, Colorado, South Dakota, New York, Florida and Montana. Meanwhile, some States like Hawaii, Pennsylvania, Mississippi, Iowa, Nebraska and Missouri have proposals that are not yet active. In contrast, Arkansas, Wyoming and Kansas are the only States that have chosen not to propose or establish any AI regulations yet.[55] The following sections present examples from selected US States and several of their adopted or proposed AI regulations. These states have taken more advanced steps in developing and implementing AI systems.[56]

A. California's Regulation

San Francisco, a city in California, became the first city in the US in 2019 to officially prohibit the use of AI facial recognition technology by law enforcement and transportation agencies. This decision was made due to concerns about risks to civil liberties, individual safety, privacy and the potential negative impact on crime prevention. Previous instances have highlighted the drawbacks and biases associated with AI, including its infringement on personal freedoms and the increased error rates when identifying women and people of colour.[57]

The *Bolstering Online Transparency Act (Senate Bill 1001)* is a law that came into effect in California in July 2019. It is primarily aimed at stopping unfair business practices and managing competition and advertising among companies online.[58] This law prohibits the use of automated online accounts (bots) that do not inform users that they are interacting with a bot, as these can influence people's opinions. It prohibits individuals and customer services from using AI bots for online engagement or communication that aims to deceive others into unknowingly servicing, buying, selling or receiving

[53] *See*, National Institute of Standards and Technology, *AI Risk Management Framework* (2023): p. 1, available at nist.gov/ai-framework, accessed on 30 March 2025.

[54] *See*, Anna M. Clark & Paula P. Plaza, "EU Artificial Intelligence Act: What Is It and How Does It Compare to U.S. AI Laws?" (2024), available at phillipslytle.com/eu-ai-act, accessed on 4 March 2025.

[55] *See*, Bryan Cave Leighton Paisner LLP, "US State-by-State Artificial Intelligence Legislation Snapshot" (2024), available at bclplaw.com/ai-snapshot, accessed on 8 April 2025.

[56] *See*, Samantha Cox, "Where AI Is Booming: Top U.S. States, Research Areas, and Industries" (2025), available at fonzi.ai/ai-hotspots, accessed on 1 December 2025.

[57] *See*, BBC News, "San Francisco is first US city to ban facial recognition" (2019), available at bbc.com/facial-ban, accessed on 8 April 2025.

[58] California Business and Professions Code §§ 17940–17943.

services. It also prohibits using AI bots to manipulate or influence individuals votes in elections.[59]

B. Illinois Regulation

Illinois AI Video Interview Act (820 ILCS 42/1/ House Bill 3773)[60] came into force in 2024 and requires that all employers who use AI systems to analyse job applicants recorded video interviews provide the applicants with information before the AI analyses their videos. There must be clear guidelines provided to the applicants stating that the employers will use AI systems to analyse the applicant video. Information and explanations regarding how the AI systems work and what they use to evaluate the applicants videos. Accurate information should be provided before the interviews and the consent of the applicants must be obtained. The employers are only allowed to share an applicants video with an expert who will be able to help evaluate the AI systems results and assist in making the decision of whether an applicant is suitable for the position. All applicants have the right to request that their interview video be deleted, and employers have up to 30 days to make sure that all the videos and copies of them are deleted within the same timeframe.[61]

C. Colorado's Regulation

Colorado has delayed the implementation of a new AI regulation, moving the date from February 2026 to June 2026.[62] This law, known as the *Colorado Artificial Intelligence Act (Senate Bill 25B-004)*[63], mirrors the focus of the EU AI Act on high-risk AI strategies, mandating that AI creators and users prioritise the rights of individuals and Colorado's security before marketing or deploying AI systems. This law aims to protect people's rights and security in Colorado from biases and discriminatory outcomes that high-risk AI systems may have on individuals or groups. Deployers who use these AI systems have the responsibility to provide their users with information about the risks and concerns they may encounter when interacting with their high-risk AI system. Especially when they are used in decision-making that may, for example,

[59] *See*, Tracy Rubin, Vince Sampson & Patrick Van Eecke, "Daily Journal Corporation: California's Bolstering Online Transparency Act targets bot disclosures in elections and transactions" (2024), available at cooley.com/ai-laws-byline, accessed on 1 December 2025.

[60] *See*, Duane Morris LLP, "Illinois Enacts Artificial Intelligence Law Focused on Employment Practices" (2024), available at duanemorris.com/illinois-ai-employment, accessed on 3 October 2025.

[61] *See*, Illinois Artificial Intelligence Video Interview Act, *820 ILCS 42/1 et seq.* (2020), available at ilga.gov/ai-video-interview, accessed on 3 October 2025.

[62] *See*, Annette Tyman & Jason Priebe, "Artificial Intelligence Legal Roundup: Colorado Postpones Implementation of AI Law as California Finalizes New Employment Discrimination Regulations and Illinois Disclosure Law Set to Take Effect", *Seyfarth Shaw LLP* (2025), available at seyfarth.com/ai-legal-roundup, accessed on 9 March 2025.

[63] *See*, Senate Bill 25B-004, *Colorado Revised Statutes §§ 6-1-1701 to 6-1-1706* (2024), available at leg.colorado.gov/ai-act, accessed on 3 October 2025.

affect an individuals education, employment, healthcare, legal and financial services, insurance, essential government services and housing.[64]

D. New York's Regulation

The State of New York was the first in the US to implement *NYC Local Law 144 of 2021*, effective since July 2023. This law forbids employers and employment agencies from using AI-driven employment decision tools unless they meet certain criteria. To legally use these AI tools in hiring, employers are required to have an independent bias audit conducted within the first year of use.[65] The audit assesses whether the AI system produces discriminatory outcomes. If algorithmic bias is identified in the first year or later, a report must be created and made public, allowing job seekers to understand how the AI tool has influenced their job applications. Violating this law can result in a civil penalty of up to $500, with subsequent fines ranging from $500 to $1,500.[66]

E. Hawaii's Proposed Regulation

In 2025, Hawaii's State Legislature put forward a bill known as *Relating to Artificial Intelligence (Hawaii Senate Bill 640)*. The purpose of this proposal is to create regulations for organisations, corporations and individual business owners using AI chatbots or similar technologies. The purpose is to ensure that these AI systems operate without disseminating misleading information and that users are made aware if they are interacting with a human or a chatbot, since AI systems are designed to mimic human behaviour and conversations. In addition, these AI chatbots collect information from users, which is subsequently sent to their developers and used to keep users engaged, often encouraging them to make purchases. Therefore, AI companies are required to provide clear and visible information so that consumers can understand with whom they are communicating, which can ultimately help ensure transparency in AI-human interactions. Violating this regulation can lead to civil penalties ranging from $1,000 to $5,000 and damages between $1,000 and $10,000.[67]

2.4 AI Regulation in China

China is a significant contributor to the advancement of AI technologies. AI is becoming a crucial component of China's digital economy, with expectations that the core industry will be worth around $150 billion by 2030. In 2017, the

[64] *See*, Stuart D. Levi et al., "Colorado's Landmark AI Act: What Companies Need To Know". *Skadden, Arps, Slate, Meagher & Flom LLP* (2024), available at skadden.com/colorado-ai, accessed on 1 December 2025.

[65] *See*, New York City AI Hiring Law, "Automated Employment Decision Tools (AEDT)", *N.Y.C. Admin. Code tit. 6, § 6-81* (2023), available at nyc.gov/aedt, accessed on 17 March 2025.

[66] Ibid.

[67] See, Hawaii Senate Bill 640, "Relating to Artificial Intelligence", *Hawaii Revised Statutes § 481B-4* (2025), available at legiscan.com/HI/SB640/2025, accessed on 3 October 2025.

Chinese government launched the New Generation AI Development Plan and by 2022, it introduced the New Generation of AI Ethics Code, which outlines both regulations and ethical guidelines for the use and advancement of AI within the country.[68] AI regulation in China is predominantly centralised and the government plays a crucial role in directing the development and application of their AI technologies.

2.4.1 An overview of some AI regulations in China

The AI regulation in the country is primarily state-controlled, emphasising content censorship and maintaining social stability to ensure that the government retains control over the development of AI technology. Currently, the government encourages AI innovation to support its strategic economic objectives. Key AI regulations are encapsulated in China's Generative AI Measures, which aim to ensure that AI systems comply with regulations such as the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law.[69] Some governance principles were introduced in 2019, and examples of two significant regulations were enacted in 2023 to govern the development and deployment of AI technologies.

Governance Principles for a New Generation of Artificial Intelligence: Develop Responsible Artificial Intelligence

In 2019, a Chinese Expert Group proposed *eight AI governance principles* aimed at fostering the sustainable and responsible advancement of AI technologies across various sectors and fields within China. These principles are crucial in ensuring the creation of safe, controllable and dependable AI systems that can support improved AI technological development.[70]

The opening *two principles* highlight that AI systems must be developed in a way that ensures individual safety and respects ethical norms, human values and rights. This later may help prevent the misuse and harmful applications of AI technology. The design and implementation process should encourage justice, fairness and equal opportunities while safeguarding the interests and rights of all stakeholders. To achieve this, it is necessary to manage and regulate AI technology by addressing biases, implementing improvements and minimising discrimination as much as possible.[71]

The *third and fourth principles* address the fact that the development of AI systems must follow environmental requirements and promote coordinated development through the upgrading and transformation of all industries in

[68] Huang et al., *supra* note 45, pp. 335–336; *See also*, Graham Webster et al., "New Generation Artificial Intelligence Development Plan, State Council of China" (2017), available at digichina.stanford.edu/ai-plan, accessed on 28 May 2025.

[69] *See*, James Gong, "What You Need to Know About China's New Generative AI Measures", *Bird & Bird* (2023); Huang et al., *supra* note 45, pp. 338–339.

[70] *See*, DigiChina Stanford University, *Governance Principles for the New Generation Artificial Intelligence: Developing Responsible Artificial Intelligence* (2019), available at digichina.stanford.edu/responsible-ai, accessed on 3 October 2025.

[71] AI Governance Principles 1–2.

China. Better education and training should be provided to the people, which can later help promote fair, open and shared competition in the development of AI. It is crucial to safeguard an individuals right to privacy by implementing additional regulations, particularly in scenarios where personal data and information may be collected, utilised and stored. Activities such as stealing, leaking, collecting or any other unlawful use of personal data and information should be strictly forbidden.[72]

Principles five and six emphasise the importance of improving trustworthiness, traceability and oversight. It is crucial to continually improve the reliability, transparency, controllability and interpretability of AI systems. The safety levels of AI systems must be maintained, enhanced and regulated. The AI developers, deployers and users must show strong self-discipline and promote social responsibility by adhering to regulations, principles, norms and standards. Penalties should be established for any violations. Users must be provided with information about the risks and impacts that these can have on individuals.[73]

The *final two principles* address the need for cross-boundary and disciplinary cooperation and exchanges to be encouraged. Collaboration among government agencies, industries, organisations, institutions in research and education must be fostered. Respect for the practices and principles of AI development mentioned above should also be considered to promote a more established international AI governance framework. Potential risks and studies must be handled to ensure that the development of AI technologies continuously benefits society.[74]

New Generation AI Development Plan and Ethics Framework

In 2023, the Cyberspace Administration of China (CAC) introduced the Interim Measures for the Management of Generative Artificial Intelligence Services.[75] This regulation, which became effective in August 2023, is a binding directive aimed at preventing AI from posing a threat to China's national security or social stability. It requires that all generative AI services accessible to the public in China adhere to core socialist values and government policies. The regulation also requires that service providers conduct security assessments and submit their algorithms to the government before making them available to the public. These provisions are intended to ensure that AI outputs remain reliable and controllable, with an emphasis on maintaining internal security and stability.[76] Penalties under this law depend

[72] AI Governance Principles 3–4.

[73] AI Governance Principles 5–6.

[74] AI Governance Principles 7–8.

[75] *See*, China Law Translate, *Interim Measures for the Management of Generative Artificial Intelligence Services* (2023), available at chinalawtranslate.com/en/generative-ai-interim, accessed on 3 October 2025.

[76] Huang et al., *supra* note 45, pp. 339–340; Interim Measures for the Management of Generative Artificial Intelligence Services, Chapter IV.

on the specific measures that have been violated, and these penalties are applied in addition to those from other applicable laws.[77]

Provisions on the Management of Deep Synthesis in Internet Information Services

The regulation in China, named the Deep Synthesis Law, which was implemented by the CAC, became effective in January 2023. The laws main focus is on addressing the risks that AI-based deepfakes, machine learning and deep learning technologies may pose online to societal safety and national security in China. AI-driven creation of content that is used in editing and generating text, audio and video is included in what is prohibited by this regulation due to the widespread occurrence of fakes and manipulations that these deepfakes may bring to society. This law places responsibility on AI developers, deployers and users in China to make sure that the AI systems are safe and designed to prevent potential misuse while, in parallel, promoting the development of transparent AI systems.[78]

[77] Interim Measures for the Management of Generative Artificial Intelligence Services, Article 21.

[78] *See*, China Law Translate, *Provisions on the Management of Deep Synthesis for Internet Information Services* (2022), available at chinalawtranslate.com/en/deep-synthesis, accessed on 3 October 2025.

Chapter 3

Fundamental Rights Approach

In this Chapter, fundamental rights are examined in relation to AI systems. The rights and freedoms addressed in this dissertation must be safeguarded against both AI systems and human actors. If a violation occurs, the owners of the AI technology bear full responsibility for any infringement carried out through their AI systems. Peoples right to privacy, data protection, non-discrimination, freedom of expression, fairness and the right to an explanation are just some of the rights that must be protected, given the potential risks associated with the development and use of AI technologies.

3.1 Human Rights Approach

Globally, numerous legal frameworks are established to safeguard and advance human rights. These frameworks encompass international conventions, protocols, declarations and recommendations. Some are *hard laws*, which hold legal authority, while others are *soft laws* that serve as advisory guidelines for member states. Upon ratifying a convention or protocol, a state is legally bound to enforce these laws and ensure the protection of human rights within its jurisdiction. These frameworks lay the groundwork for managing the implications of emerging technological advancements and human-robot interactions.[79]

Human rights are protected by multiple international laws, many of which are maintained by the Office of the United Nations High Commissioner for Human Rights (OHCHR). Three principal documents, known collectively as the *International Bill of Human Rights*, include the International Covenant on Civil and Political Rights (ICCPR)[80], the International Covenant on Economic, Social and Cultural Rights (ICESCR)[81] and the Universal Declaration of Human Rights (UDHR)[82].[83] While the first two covenants are legally binding

[79] *See*, *DagDok*, *International Law - Conventions and Declarations* (2025), available at dagdok.org/un-law, accessed on 9 October 2025.

[80] *See*, United Nations, *International Covenant on Civil and Political Rights, 999 U.N.T.S. 171* (1966), available at ohchr.org/iccpr, accessed 20 on June 2025.

[81] *See*, United Nations, *International Covenant on Economic, Social and Cultural Rights, 993 U.N.T.S. 3* (1966), available at ohchr.org/icescr, accessed on 20 June 2025.

[82] *See*, United Nations, *Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810* (1948), available at un.org/udhr, accessed on 20 June 2025.

[83] *See*, United Nations, *International Bill of Human Rights* (1996). available at ohchr.org/bill-of-rights, accessed on 18 June 2025.

for countries that have ratified them, the UDHR is not legally enforceable and serves as a doctrinal declaration providing guidelines for the respect and protection of human rights globally.[84] The EU, the US, and China have either signed, implemented or adopted various portions of the international regulations mentioned above.

3.1.1 EU's Rights Approach

Within the EU, the safeguarding of individuals fundamental rights is primarily upheld by two key regulations.[85] The. These include the EU Charter of Fundamental Rights (Regulation (EU) 2000/C 364/01) and the European Convention on Human Rights (ECHR), both of which provide robust protection for personal rights across the EU and Europe.[86] These laws are obligatory for all EU member states,[87] which have imposed a significant duty on them to implement these regulations at the national level. Such implementation is crucial to ensure the protection of fundamental rights within their jurisdictions. In addition, other regulations are in place to specifically protect certain rights.[88] There are also other regulations in place that specifically focus on protecting some rights outlined in the ECHR and the EU Charter of Fundamental Rights. These regulations are designed to ensure that the safety, freedoms and fundamental rights of individuals are protected, especially in the context of using AI systems.

In 2024, the Council of Europe introduced the first globally legally binding agreement on AI, known as the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (Framework Convention (CETS No. 225)), which has been available for signing since September 2024.[89] The purpose of this convention is to uphold vital international standards and objectives to address the legal gaps necessary for protect human rights, democratic principles and the rule of law amidst the rapid advancement of AI technologies.[90] Several Council of Europe and EU member states have signed this treaty, along with a few other nations such as the US, Israel, Japan and Canada. To bring this treaty into effect, it requires ratification by five countries, of which three must be Council of Europe members.[91]

[84] DagDok, *supra* note 79.

[85] *See*, Paul Craig & Gráinne de Búrca, *EU Law: Text, Cases, and Materials*, 8th edn, Oxford University Press (2024): p. 409.

[86] *See*, EU Charter of Fundamental Rights, *Regulation (EU) 2000/C 364/01* (2000), available at fra.europa.eu, accessed on 4 May 2025; *See also*, European Convention on Human Rights, *ETS No. 005* (1950), available at echr.coe.int, accessed on 4 May 2025.

[87] *See*, European Union, Types of EU Legislation (2024), available at europa.eu/eu-legislation, accessed on 1 May 2025.

[88] TFEU, Article 6; EU Charter of Fundamental Rights, *supra* note 86.

[89] *See*, Council of Europe, "Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law" (2024), available at coe.int/ai-convention, accessed on 3 May 2025.

[90] CETS No. 225, Article 1.

[91] CETS No. 225, *supra* note 89.

The Framework Convention comprises 36 Articles organised into 8 Chapters based on their content.[92] Once this Convention is enacted, states will be obligated to implement it to uphold the protection of individual rights and to reduce the risks and impacts of AI systems in both public and private sectors. There are exceptions allowing countries not to adhere to this Convention when they need to protect national security, provided this is done in accordance with international law.[93] Ensuring the protection of individual rights to equality, non-discrimination, privacy and data protection in the context of AI system usage is paramount. Transparency, responsibility, oversight and accountability are essential measures to ensure that human rights, democracy and the rule of law are respected by AI developers and deployers.[94]

3.1.2 US Rights Approach

The protection of individual's fundamental rights and freedoms in the US is primarily secured through the Bill of Rights, the collective name for the first Ten Amendments in the U.S. Constitution. Ratified in 1791, these Amendments establish strong federal protections for fundamental freedoms and due process rights. They are legally binding across all federal and state jurisdictions and impose a substantial obligation on all US authorities to respect and enforce these constitutional guarantees in order to ensure the protection of fundamental rights within US territory. The U.S. Constitution establishes a minimum level of protection for individual rights, states may provide stronger protections or additional rights, so long as they do not conflict with federally protected rights or other federal regulations.[95]

3.1.3 Chinas Rights Approach

Certain safeguards for individual rights in China are set out in Chapter II of the Chinese Constitution, which focuses on the fundamental rights and duties of citizens. These articles of the Constitution establish fundamental civil and political rights, as well as some social and economic protections for individuals in China.[96] Furthermore, Book Four of the Civil Code of the People's Republic of China sets out more detailed rules on the protection of personality rights and other aspects of individual dignity.[97] Together, the Constitution and the Civil Code form a legal framework that aims to safeguard citizen's lawful rights and interests in China.

[92] Ibdi.

[93] CETS No. 225, Chapters I and II.

[94] CETS No. 225, Chapter II.

[95] *See*, The U.S. National Archives and Records Administration, *United States Bill of Rights* (1791), available at archives.gov/bill-of-rights, accessed on 3 December 2025.

[96] *See*, Constitution of the People's Republic of China (1982), available at npc.gov.cn/constitution, accessed on 3 October 2025.

[97] *See*, WIPO Lex, *Civil Code of the People's Republic of China* (2020), Book One, Chapter I, available at wipo.int/china-civil-code, accessed on 3 December 2025.

3.2 Individuals Right to Privacy and Data Protection

In the digital age, the traditional right to privacy faces unprecedented challenges from large-scale data collection and AI-driven surveillance. Both Article 17 of the ICCPR and Article 12 of the UDHR state that individuals have the right to privacy in their home, family life and communications, a protection that now clearly extends to the misuse of personal data and AI-based surveillance. Attacks on a person's honor or reputation are forbidden and governments are required to implement laws to protect individuals from unwarranted or unlawful interventions in their privacy, whether online or offline. In this context, AI systems that handle personal data without consent or a clear legal basis are not allowed.[98]

3.2.1 EU's Privacy and Data Protection Regulations

Within the EU, regulations exist to protect personal privacy and data protection both online and offline, as well as in contexts involving AI systems. These regulations aim to protect an individual's safety, fundamental rights and freedoms from being compromised during the development, deployment and use of AI systems. Together, Article 7 and Article 8 of the EU Charter of Fundamental Rights, along with Article 8 of the ECHR, form the core legal framework for privacy and data protection in this area.

Article 7 of the EU Charter of Fundamental Rights states that everyone has the right to be respected and protected in their home, family life and private communications. These protections apply to individuals in both the physical and digital spheres. Technological intrusions into privacy, such as AI deepfakes, data collection or biometric surveillance, are forbidden.[99]

Building on this, Article 8 of the EU Charter of Fundamental Rights focuses specifically on personal data. Every individual is entitled to the safeguarding of their personal information. This data must be handled in a lawful, fair and transparent manner, even when AI systems are involved. Prior to any data processing, individuals need to be fully informed about how their data will be used and must provide explicit consent. Individuals have the right to access, amend or request the removal of their personal data from both automated systems and AI training databases. People must have the ability to contact the data controllers and application operators of AI systems that are processing their information. It is the responsibility of independent supervisory authorities to monitor and ensure compliance with these regulations.[100]

Similarly, Article 8 of the ECHR protects private and family life in a way that also covers AI-related risks Each person is entitled to respect for their private and family life, home and communications, including protection

[98] ICCPR, Article 17; UDHR, Article 12.
[99] EU Charter of Fundamental Rights, Article 7.
[100] EU Charter of Fundamental Rights, Article 8.

from invasive AI systems. Public authorities should not disrupt this right, whether via conventional methods or AI technologies, unless it is absolutely necessary in a democratic society. Exceptions are made in cases where national security, public safety or crime prevention are under threat. Laws need to be established to limit AI surveillance and ensure individuals are informed when AI systems utilise or store their data. These measures are essential to uphold the individual's right to privacy and family life.[101]

Taken together, these provisions ensure that both traditional forms of interference and new AI-driven practices are subject to strong privacy and data protection safeguards in Europe. Against this background, the EU's General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)[102] plays a central role in shaping how personal data is processed in AI-driven contexts. In the EU, the cornerstone of data protection law is the GDPR, which provides the primary legal framework governing the processing of personal data, including in relation to AI systems.

The GDPR came into force in May 2018 and is one of the most important regulations regarding the protection of individuals' personal data and their right to privacy within the EU. While the regulation does not explicitly reference AI systems, there are still specific guidelines that AI developers and implementers need to adhere to in order to comply with the regulation. This regulation aims to ensure ethical AI development by emphasising the significance of privacy and data protection.[103]

The core principles for the collection and processing of an individual's personal data by either a person or AI systems are outlined in Articles 5 and 6 of the GDPR. These articles mandate that personal data must be processed in a lawful, fair and transparent manner.[104] Moreover, an individual's personal data should only be gathered for purposes that are specific, clearly defined and lawful, with the individual's consent being required.[105] Exceptions to these conditions, such as for scientific research, are allowed only if they respect the fundamental rights and freedoms of individuals.[106]

Taken together, these principles not only govern how personal data may be collected and used, but also shape the concrete rights afforded to data subjects. Citizens within the EU are therefore entitled to receive information about how their personal data is processed online and in situations where AI is involved. In line with the requirement of lawfulness, fairness and transparency, they also have the right to retract their consent regarding data use and the right to be forgotten, allowing them to request the deletion of their data from online services or platforms.[107] These individual rights are backed by a robust enforcement framework. Breaches of the GDPR are subject to prosecution at

[101] ECHR, Article 8.

[102] *See*, General Data Protection Regulation, *Regulation (EU) 2016/679 (2016)*, Article 99, available at eur-lex.europa.eu/gdpr, accessed on 9 March 2025.

[103] *See*, DLA Piper, "Europe: The EU AI Act's Relationship with Data Protection Law: Key Takeaways" (2024), available at dlapiper.com/ai-act-dp, accessed on 30 May 2025.

[104] GDPR, Recitals 39–40; Azam, *supra* note 10, p. 91.

[105] GDPR, Articles 13–14.

[106] GDPR, Article 89.

[107] GDPR, Articles 17 and 21.

the EU Court of Justice. If a GDPR violation is confirmed, the responsible entity may face civil and financial penalties. Affected individuals have the right to seek compensation for damages and supervisory bodies have the authority to impose administrative fines of up to €20 million or more, varying according to the violation of the Articles in the regulation.[108]

3.2.2 US Privacy and Data Protection Regulations

In the United States, there is no comprehensive, specific or clearly defined privacy and data protection regime at the federal level. Instead, data protection is addressed through a patchwork of sectoral rules and state-level legislation. In response to these gaps, a growing number of states have enacted their own privacy statutes, each seeking to enhance the protection of individuals' personal data within its jurisdiction.[109] The following sections discuss two illustrative states, each of which has adopted its own privacy and data protection framework.

The Texas Data Privacy and Security Act (TDPSA) (House Bill 4), which took effect in 2024, establishes a comprehensive framework for protecting individuals' personal information and data in Texas.[110] The TDPSA grants Texas consumers a series of rights designed to increase transparency and control over their data, including the right to understand how their data are collected, used, sold, analysed, stored, and retained by businesses operating in the state. Covered entities must disclose these practices in a clear and accessible manner and obtain consumer consent before collecting sensitive personal data. Where a business intends to sell personal or biometric data, it must provide a prominent notice, such as: "*NOTICE: We may sell your sensitive personal data or biometric data*." Each violation of this law can result in a penalty of up to $7,500.[111]

The California Consumer Privacy Act of 2018 (CCPA) is a law that was enacted in the state of California in 2020 to protect the privacy and personal data of California residents.[112] This regulation grants Californians the right to be informed and to have control over their personal data when it is being collected by businesses, third parties and AI technologies. This imposes obligations on AI developers and third parties to provide consumers with clear information regarding the use and sharing of their personal information and data.[113] In 2023, an amendment known as the California Privacy Rights Act of 2020 (CPRA) was introduced to further strengthen the CCPA.[114] The

[108] GDPR, Articles 82–84.

[109] *See*, DLA Piper, "Data protection laws in the United States" (2025), available at dlapiperdataprotection.com/us, accessed on 3 October 2025.

[110] *See*, Texas Data Privacy and Security Act, *Texas Business & Commerce Code §§ 541.001–541.155* (2023), available at dir.texas.gov/tdpsa, accessed on 29 September 2025.

[111] Texas Business & Commerce Code §§ 541.155.

[112] *See*, California Consumer Privacy Act, *California Civil Code §§ 1798.100–1798.198* (2018), available at thecpra.org, accessed on 3 October 2025.

[113] California Civil Code § 1798.100.

[114] *See*, California Privacy Rights Act, *California Civil Code §§ 1798.100–1798.199.100* (2023), thecpra.org, accessed 30 May 2025.

CPRA enhances privacy and data security measures for California residents by giving them the right to restrict the use and collection of their personal data. Together, these regulations impose fines for violating the CCPA and CPRA, with penalties of $2,500 per breach and up to $7,500 for intentional violations, and in cases of data breaches, compensation ranging from $100 up to $750 per affected consumer.[115]

3.2.3 China's Privacy and Data Protection Regulations

In China, every individual's right to privacy and personal information is outlined in Book 4, Chapter VI of the Civil Code, which prohibits individuals, organisations and AI systems from violating this right. Such violations occur where an individual's privacy or personal information is invaded, exposed, trespassed upon or revealed without that person's consent. This right may only be infringed in circumstances permitted by law or where the right holder has expressly agreed.[116]

China's main data protection statute, the Personal Information Protection Law of the People's Republic of China (PIPL),[117] has been in force since 1 November 2021. It oversees the safeguarding and management of personal data both within China and in cross-border contexts, and requires that personal information be processed in a lawful, ethical and proper manner, without deception, coercion or fraud. When personal data is collected by either natural persons or AI systems, the processing must be limited to what is necessary and must comply with the principles of transparency and openness.[118]

Chapter 2 of the PIPL specifies the circumstances in which personal information may be processed by companies, individuals and AI systems. These include situations in which the data subject has given consent, public health emergencies or other crises, matters involving the protection of life, health or property, contract performance, the conduct of public affairs, news reporting and other public interest activities, the handling of information that has been lawfully disclosed, and the performance of statutory duties.[119]

In addition, the PIPL recognises that in some situations personal information may be processed without obtaining the individual's consent, as provided for in administrative regulations, other laws and judicial interpretations.[120] Individuals retain the right to access, copy and manage their personal information and to be informed about how it is used. Subject to legal exceptions,[121] they may refuse, restrict or request the deletion of the processing of their personal data.[122] Non-compliance with the PIPL can result

[115] California Civil Code §§ 1798.150 and 1798.155.

[116] Civil Code of the People's Republic of China, Articles 1032 and 1034.

[117] *See*, Personal Information Protection Law of the People's Republic of China (2021), available at pip-law.com, accessed on 3 December 2025.

[118] PIPL, Chapter 1.

[119] PIPL, Chapter 2.

[120] PIPL, Article 13(2 and 7).

[121] Ibid.

[122] PIPL, Chapter IV.

in significant penalties, including fines of up to RMB 50 million or 5% of a company's turnover from the previous year.[123]

3.3 Individuals Right to Non-Discrimination

All individuals, wherever they may be, are entitled to the fundamental rights and freedoms set out in the UDHR and the ICCPR, without any discrimination. These guarantees apply equally whether discrimination is carried out by a person, an institution or an algorithmic or technological AI system.[124]

No one may be deprived of their rights on the basis of race, colour, sex or gender, language, religion, political or other opinion, nationality, social origin, economic or social status, place of birth or any other attribute or status. This prohibition covers not only direct human conduct, but also situations in which AI systems inaccurately assess or classify individuals because of biased data, flawed design or discriminatory deployment.[125]

Each State Party to the ICCPR must respect and ensure these rights to all individuals within its territory and jurisdiction, and must adopt legislative, administrative and other measures to protect individuals from discrimination, including AI-driven infringements in areas such as employment, access to loans and other financial services, policing, social services, legal decision-making, and access to essential services. No territorial or political status may be invoked to justify discrimination, whether through traditional means or through automated AI systems that disproportionately disadvantage marginalised communities.[126]

Where rights protected under the UDHR and ICCPR are violated, every affected person must have access to an effective remedy. This includes the ability to challenge and seek review of algorithmic and other AI-generated decisions before an independent authority or court, and to obtain appropriate redress where a violation is established. In all such contexts, everyone is entitled to equal protection of and before the law, without exception.[127] Building on these general protections, specific human rights treaties further clarify State's obligations in relation to discrimination.

The International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) comprises 25 Articles and underscores the global initiative to prohibit and abolish all forms of racial discrimination, including apartheid and segregation. It advocates for dignity and equality by upholding the rights outlined in the UDHR.[128] Approximately 182 nations worldwide

[123] PIPL, Article 66.
[124] UDHR, Article 2; ICCPR, Articles 2 and 26.
[125] Ibid.
[126] ICCPR, Articles 2 and 26.
[127] Ibid.
[128] *See*, United Nations, *International Convention on the Elimination of All Forms of Racial Discrimination, 660 U.N.T.S. 195* (1969), available at ohchr.org/cerd, accessed 1 December 2025.

have ratified the convention, including EU countries, the US and China, which then have the obligation to make sure that the convention is being followed.[129]

In the context of AI regulation, the three chapters containing articles in the ICERD can be linked to the responsibilities that AI technology developers and employers have in ensuring that AI systems do not perpetuate or reinforce racial discrimination. This requires them to implement strategies in order to eliminate biases in the AI algorithms that could potentially cause discriminatory outcomes and to ensure that all AI systems respect the dignity and equality of all individuals, in alignment with the regulation. The commitment to the convention by leading AI developers such as the EU, the US, and China may result in effective AI regulations that prevent racial discrimination, promoting technologies that contribute to an international community free from racial segregation and discrimination.

3.3.1 EU's Non-Discrimination Regulations

The EU's legal framework strictly prohibits all forms of discrimination, whether arising from human actions or from AI systems. This prohibition covers grounds such as sex, race, colour, ethnic or social origin, genetic traits, language, religion or belief, political or other opinions, membership of a national minority, property, birth, disability, age or sexual orientation. EU member states are required to adopt and enforce measures that effectively protect individuals against biased or discriminatory outcomes produced by AI systems, particularly in areas such as employment, algorithmic profiling and other automated decision-making processes.[130]

Building on these EU-level guarantees, Article 14 of the ECHR similarly requires that all rights and freedoms set forth in the Convention be secured without discrimination, whether violations stem from human conduct or from AI systems. The prohibited grounds include, among others, sex, race, colour, language, religion, political or other opinions, national or social origin, association with a national minority, property, birth or other status. States have a positive obligation to adopt and enforce legal safeguards so that AI systems cannot be used to circumvent these non-discrimination guarantees.[131]

Complementing these non-discrimination provisions, Article 22 of the GDPR provides individuals with specific protections against decisions based solely on automated processing, including profiling, where such decisions produce legal effects concerning them or similarly significantly affect them. In practice, this imposes duties on AI developers and deployers to design and operate AI systems in a way that respects transparency, fairness, accountability and non-discrimination. Individuals must be able to challenge automated

[129] *See*, Office of the United Nations High Commissioner for Human Rights, "Status of Ratification Interactive Dashboard" (2025), available at indicators.ohchr.org, accessed on 1 December 2025.

[130] TFEU, Articles 19 and 157; EU Charter of Fundamental Rights, Articles 20–21.

[131] ECHR, Article 14.

decisions, obtain meaningful information about the logic involved and seek human intervention where necessary to protect their fundamental rights.[132]

These protections are closely linked to the work of equality institutions within the EU framework. *Equality bodies* in the EU are independent public organisations with the goal of helping EU member states implement the three central equality directives, which play a crucial role in promoting equal treatment and combating discrimination against individuals within the EU.[133] Their mandates are increasingly relevant not only in personal interactions but also in protecting individual rights in the context of algorithmic and AI-driven decision-making, where they can support enforcement of non-discrimination guarantees and oversee the handling and deployment of AI systems.

Central equality regulations in the EU are the Racial Equality Directive[134], the Gender Equality Directive[135] and the Employment Equality Directive[136], each focused on potential biases related to race, age, religion, disability, gender and sexual orientation. Taken together, these instruments also place the burden on AI developers to ensure that their AI systems are designed in accordance with these directives and other EU regulations, aiming to prevent discrimination and promote fairness, transparency and accountability. To successfully implement these laws in the AI context, it is important to ensure that AI training data are inclusive and balanced by addressing and striving to reduce current biases.[137]

In addition to data design, regular inspections and evaluations of AI systems should be performed to maintain fairness and transparency, allowing AI researchers to detect and address any indicators of algorithmic bias or discriminatory outcomes. Finally, education and awareness play a crucial role in increasing public understanding of AI technologies and the impact these AI systems may have on society when they are developed and used in both public and private settings.[138]

3.3.2 US Non-Discrimination Regulations

In the US, there are laws at both the federal and state levels that prohibit unlawful discrimination and bias in both private and public spheres. The 14th Amendment of the U.S. Constitution contributes to preventing discriminatory practices and highlights the importance of equal treatment nationwide.[139] In particular, federal civil-rights legislation such as the Civil Rights Act of 1964

[132] GDPR, Article 22.

[133] *See*, European Commission, "Equality Bodies" (2024), available at commission.europa.eu/equality-bodies, accessed on 1 December 2025.

[134] *See*, Racial Equality Directive, *Directive (EU) 2000/43/EC* (2000), available at Summary and Official Journal, accessed on 1 December 2025.

[135] *See*, Gender Equality Directive, *Directive (EU) 2006/54/EC* (2006), available at eur-lex.europa.eu/gender-equality, accessed on 1 December 2025.

[136] *See*, Employment Equality Directive, *Directive (EU) 2000/78/EC* (2000), available at eur-lex.europa.eu/employment-equality, accessed on 1 December 2025.

[137] European Commission, *supra* note 133.

[138] Ibid.

[139] *See*, United States Constitution, *The Amendments* (1791–1992), Amendment XIV, available at constitutioncenter.org/amendments, accessed on 30 May 2025.

and the Americans with Disabilities Act (ADA) established in 1990, plays a central role in safeguarding individuals from discrimination and bias.

Building on the constitutional guarantee of equal protection, the Civil Rights Act is a crucial federal regulation that protects worker's rights by prohibiting discrimination or bias within the workplace by employers, other individuals and even AI systems. This legislation safeguards against discrimination based on race, religion, colour, national origin, pregnancy, sex, sexual orientation, gender and gender identity.[140] Likewise, the ADA regulation is an important law that protects individuals with disabilities from discrimination and bias, ensuring their rights in both employment settings and public life.[141]

Together, these federal laws impose a significant obligation on AI developers, companies, employers and states to ensure that AI systems used in workplaces, public spaces and during hiring processes do not breach these legal standards. In practice, this means that AI technologies must undergo safety tests prior to deployment and inspections during their use. The Equal Employment Opportunity Commission (EEOC) is responsible for investigating and ensuring compliance with these laws and other regulations in this sphere.[142]

3.3.3 China's Non-Discrimination Regulations

In China, regulations concerning non-discrimination are distributed across various laws. The Constitution includes certain anti-discrimination laws, asserting that all citizens are equal under the law and safeguarding voting rights, free speech and the interests of religious and ethnic groups, although it does not specifically mention sexual orientation or other statuses.[143] The constitutional protections against discrimination are also relevant to the creation and application of AI systems, given the potential risks and discriminatory impacts that AI technology may have on individuals or groups.

Building on these general constitutional guarantees, the Employment Promotion Law of 2007 provides more specific protections in the labour context. It ensures that every worker has the right to protection from discrimination and bias related to race, nationality, religion, gender and disability. These safeguards are particularly important when AI systems are employed in recruitment and workplace settings. In other words, any type of bias or discriminatory behaviour by an individual or an AI system in the workplace is prohibited.[144]

[140] *See*, Civil Rights Act of 1964, *Title VII, 42 U.S.C. §§ 2000e–2000e-17* (1964), available at eeoc.gov/title-vii, accessed on 1 October 2025.

[141] *See*, Americans with Disabilities Act of 1990, *42 U.S.C. §§ 12101–12213* (1990), available at ada.gov, accessed on 1 October 2025.

[142] *See*, U.S. Equal Employment Opportunity Commission, "Enforcement Guidance on Harassment in the Workplace" (2023), available at eeoc.gov/overview, accessed on 3 October 2025.

[143] Constitution of the People's Republic of China, Articles 4 and 33–36.

[144] *See*, Employment Promotion Law of the People's Republic of China (2007), Articles 3 and 26, available at cecc.gov/employment-promotion-law, accessed on 3 October 2025.

In addition to the Constitution and the Employment Promotion Law, data protection legislation also addresses discriminatory risks from AI. Article 24 of the PIPL prohibits AI systems that cause discrimination, even when used in automatic decision-making processes. The AI system used within this sector must be fair and transparent in order to prevent algorithmic harm, bias or other discriminatory outcomes when making decisions that may affect an individual's interests and rights. This places responsibility on AI developers and deployers to ensure their systems comply with laws and thereby enhance accountability within AI systems.[145]

3.4 Individuals Right to Freedom of Expression

At the international level, every individual has the right to hold and express their opinions without interference from other individuals, States or AI systems. Everyone should be able to freely seek, receive and share information and ideas, both online and offline and through any media or form of communication, including digital platforms using AI systems, as well as written, printed, artistic or other media formats.[146]

These freedoms must not be infringed upon by AI systems through surveillance, censorship, manipulation or other forms of interference. At the same time, every State has the responsibility to adopt regulations to prevent illegal activities and may impose restrictions on the exercise of this right only where necessary and proportionate to protect national security, public order, public health or public morals. Such restrictions also pertain to the design, deployment and use of AI systems.[147]

3.4.1 EU's Freedom of Expression Regulations

In the EU, every individual is guaranteed the right to freedom of expression and information under Article 11 of the EU Charter of Fundamental Rights. They have the right to express their thoughts about AI systems, receive information when these systems might impact them and disseminate their AI-related knowledge without interference from public authorities or across borders, in line with the protection of this right.[148]

Similarly, under Article 10 of the ECHR, all individuals have the right to freedom of thought and expression, as well as the ability to receive and disseminate information without interference from government bodies or AI systems. However, there are circumstances in which governments may impose restrictions and regulations to safeguard national security, public safety, health, morals, laws or other requirements deemed essential in a democratic society. According to Article 10, such restrictions can, in theory, be applied with the assistance of AI systems, provided they adhere to these exceptions.[149]

[145] PIPL, Article 24.
[146] ICCPR, Article 19; UDHR, Article 19.
[147] Ibid.
[148] EU Charter of Fundamental Rights, Article 11.
[149] ECHR, Article 10.

3.4.2 US Freedom of Expression Regulations

The First Amendment of the U.S. Constitution states that no law shall be passed by Congress that infringes on people's rights to free speech, a free press, freedom of religion and religious practice, peaceful assembly or to petition the government to address injustices caused by other individuals or AI systems.[150]

3.4.3 China's Freedom of Expression Regulations

All citizens of China have the right to freedom of speech, demonstration, assembly, press, procession and association, thereby giving them the right to express their views on AI systems.[151]

3.5 Individuals Right to Fairness and Explanation

Under International Human Rights Law, Articles 7 and 10 of the UDHR and Article 14 of the ICCPR guarantee that all individuals are entitled to equal treatment under the law and must not face any discrimination regarding equal legal protection. In particular, they require that everyone enjoys full equality in the right to a fair and public hearing by an independent and impartial tribunal. These guarantees apply irrespective of whether legal processes are conducted entirely by humans or involve the use of AI systems.[152]

Accordingly, the judiciary must maintain its independence and impartiality at all times, regardless of whether judgments are delivered solely by human decision-makers or supported by AI tools. Where AI is employed in legal proceedings, its deployment must be governed by rigorous guidelines that preserve these fundamental guarantees. In particular, AI systems must be sufficiently transparent to enable individuals to understand, in clear terms, how conclusions are reached, and there must be accessible and effective procedures for contesting decisions that are made or influenced by AI.[153]

3.5.1 EU's Fairness and Explanation Regulations

Across the EU legal framework, several key provisions jointly safeguard fairness, transparency and the right to an explanation in contexts where AI systems may affect individual's rights.

Article 47 of the EU Charter of Fundamental Rights guarantees that anyone in the EU whose rights and freedoms are violated, whether by an individual or an AI system, has the right to a meaningful court hearing. Such a hearing must be fair and public, take place within a reasonable time frame, and be conducted by a neutral and impartial tribunal established by law. Where individuals lack sufficient resources, support must be provided to ensure

[150] U.S. Constitution, Amendment I.
[151] Constitution of the People's Republic of China, Article 35.
[152] ICCPR, Article 14; UDHR, Articles 7 and 10.
[153] Ibid.

effective access to justice. These safeguards apply equally when AI systems are used in legal processes, case management or decision support.[154]

Complementing Article 47, Article 41 of the EU Charter of the Fundamental Rights focuses on the right to good administration by EU institutions. Individuals are entitled to have their issues processed fairly and efficiently, including when AI systems are used by EU bodies. Such systems must comply with principles of fairness and transparency and be designed to uphold individual's rights to be heard and to receive an explanation or justification before or after any AI-based decision that may affect them. Where actions of EU institutions or their AI systems cause harm, affected individuals are entitled to compensation.[155]

Article 6 of the ECHR reinforces these guarantees by enshrining the right to a fair trial. If AI systems are integrated into judicial processes, they must be evaluated and supervised to ensure compliance with the principles of privacy, justice, transparency, impartiality and the presumption of innocence until proven guilty in court. The role and use of AI in proceedings must be clear and must not undermine the protection of individual rights.[156]

Finally, Article 5(1)(a) of the GDPR addresses fairness and transparency in the processing of personal data, which is often central to AI systems. All personal data must be processed lawfully, fairly and transparently, with clear information provided to individuals about how their data are collected, used, processed and accessed by companies, other individuals or AI systems.[157]

Taken together, these instruments outline a coherent regulatory framework that requires AI systems used in the EU to respect fair trial guarantees, good administration, and transparent, fair data processing, while ensuring that individuals can understand and challenge AI-driven decisions that affect them.

3.5.2 US Fairness and Explanation Regulations

The 14th Amendment of the U.S. Constitution is strongly linked to concepts of fairness and explanation within the AI industry, owing to its commitment to fair procedures and equal rights. It highlights the importance of just legal procedures, which parallels the need for transparency and fairness in AI decision-making. When AI systems are introduced in the justice or public administration sectors, they must ensure consistent, unbiased outcomes and impartial results, while also providing those affected with enough information to understand and contest AI decisions. In addition, the Amendment guarantees the right to equal protection, forbidding states from denying equal legal protection to anyone within their jurisdiction. Accordingly, for AI systems to be employed, they must be designed, maintained, and operated

[154] EU Charter of Fundamental Rights, Article 47.
[155] EU Charter of Fundamental Rights, Article 41.
[156] ECHR, Article 6.
[157] GDPR, Article 5(1)(a) and Recital 39.

without algorithmic bias in their decision-making processes, in line with individuals' rights to fairness and explanation.[158]

3.5.3 China's Fairness and Explanation Regulations

Every individual who holds Chinese citizenship is guaranteed their rights as specified in the regulations and everyone is equal under the law. It is the state's duty to safeguard and respect people's rights. In contrast, citizens are obligated to adhere to and fulfill the responsibilities outlined in the Constitution and regulations.[159]

Firstly, Articles 4–6 of the Civil Code clarify that AI developers and operators have the responsibility to ensure that their AI systems follow the principles of fairness, equality and freedom. This implies that AI systems should be designed to guarantee equal treatment, enable users to make informed decisions regarding their interactions, and ensure that AI technologies engaging with individuals are fair, transparent and accountable for any negative impacts they might have on a person.[160]

Furthermore, Article 24 of the PIPL strengthens these fairness obligations by granting individuals the right to request explanations, access and control over decisions made by AI systems that could impact them. This provision increases the obligations of AI developers and operators to create AI systems that are more transparent and fair, particularly when these systems are used for decision-making processes that could significantly affect a person's fundamental rights, such as handling their personal data or infringing on their right to non-discrimination.[161]

[158] U.S. Constitution, Amendment XIV.
[159] Constitution of the People's Republic of China, Article 33(2–4).
[160] Civil Code, Articles 4–6.
[161] PIPL, Article 24.

Chapter 4

Balances and Obstacles

At present, there are virtually no reported legal cases specifically addressing violations involving artificial intelligence technologies. This is largely because many of the relevant regulatory frameworks have only recently been enacted or are still under development and the field itself is comparatively new. As a result, it may be several years before a substantial body of case law emerges, once these regulations fully enter into force and are tested in courts. In the meantime, it is difficult to identify the precise balances, challenges and limitations of AI regulation, because higher courts and key institutions have not yet had the opportunity to interpret these laws and clarify how they should be applied in practice. Nevertheless, this does not give AI developers, deployers or users the right to violate people's fundamental rights through the use of AI technologies. In this Chapter are some examples of key benefits, balancing acts and obstacles associated with AI regulation in the EU, the US, and China.

4.1 Balances of the EU AI Regulation

The EU AI Act aims to safeguard ethical values and fundamental rights within the Union by classifying AI systems into four risk levels and imposing corresponding obligations, including strict prohibitions on certain practices and extensive requirements for high-risk AI systems, which are detailed in Articles 5–6 of the EU AI Act. These obligations apply to providers, deployers and other relevant actors who place AI systems on the EU market or use them within EU territory to make sure that their AI systems comply with EU regulations and effectively enhance the protection of EU citizens fundamental rights.[162] EU member states must designate or establish national competent authorities to supervise compliance and cooperate with EU-level bodies, thereby reinforcing a coherent, rights-based enforcement architecture across the Union.[163] Non-compliance may result in significant administrative fines and provider penalties that are intended to have a strong deterrent effect and

---

[162] *See*, European Parliament, "Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI" (2023), available at europarl.europa.eu/ai-act-deal, accessed on 19 November 2025.

[163] EU AI Act, Article 77.

to secure meaningful remedies for individuals whose rights are adversely affected.[164]

Important provisions found in Articles 77 and 27 of the EU AI Act outline structures and assign responsibility to national public authorities or bodies in the region, under which AI developers and deployers are required to ensure that their high-risk AI systems, developed or implemented in the EU, are harmonised and align with the fundamental rights protections laid out in the EU Charter of Fundamental Rights, the ECHR and other EU hard laws that protect people's rights.[165] These provisions also grant people in the EU the right to know what AI systems are designed to do, the types of decisions they produce and how those systems may influence results, thereby strengthening individuals ability to contest decisions and exercise their rights in practice.[166]

Article 27 imposes a transparency obligation by requiring Fundamental Rights Impact Assessments (FRIA) for high-risk AI systems. These assessments must disclose the purpose of the AI technologies, the criteria used in their decision-making and the risks they pose to fundamental rights, thereby supporting accountability and safeguarding the protection of rights.[167] Every EU member state has under the EU AI Act, a national authority responsible for protecting people's fundamental rights in the context of AI. These authorities have specific investigative and enforcement powers, enabling them to act where AI systems infringe or risk infringing fundamental rights. Each member state must draw up and publish a list of the authorities or bodies entrusted with this role when implementing the EU AI Act.[168] Against this institutional backdrop, FRIA becomes an fundamental instrument, because it helps find and reduce possible harms before an AI system is used. In doing so, it makes sure AI is developed and used in ways that respect human rights and ethics, and it builds a proactive, rights-based risk check into how AI is governed. As these AI systems become increasingly influential in sectors such as healthcare, law enforcement and employment, FRIA provides a structured framework to promote transparency, non-discrimination and compliance with EU legal standards, while also giving national authorities the information they need to supervise the use of high-risk AI systems and, where appropriate, to assess and intervene.[169]

Taken together, these mechanisms demonstrate how the EU AI Act functions as a centralised and explicitly rights-based regulation that seeks to balance the development and uptake of AI technologies with robust safeguards designed to ensure a fundamental rights-oriented regulatory framework, contributing to AI systems that are safer, more trustworthy, fair,

[164] EU AI Act, Articles 99–101.

[165] EU AI Act, Articles 77 and 27.

[166] EU AI Act, Recitals 93 and 96.

[167] *See*, Thomas Ajoodha & Jared Browne, "Fundamental Rights Impact Assessments: What Are They? How Do They Work?", *CEDPO AI and Data Working Group Micro-Insights Series* (2025), available at cedpo.eu/micro-insight, accessed on 5 April 2025.

[168] *See*, European Commission, "Fundamental Rights Protection and Authorities Under the AI Act" (2024), available at digital-strategy.ec.europa.eu/fundamental-rights-ai, accessed on 3 December 2025.

[169] Ajoodha & Browne, *supra* note 167.

transparent and accountable to the individuals whose rights they affect before they are released for use.

4.1.1 Fundamental Rights and the EU AI Act: Practical Obstacles and Critical Reflections

While the EU AI Act provides a comprehensive framework aimed at ensuring compliance of high-risk AI systems with the individual fundamental rights, the practical realisation of these aims encounters several significant obstacles where legal, institutional and technical challenges occur which may undermine the effective protection of the practical application of fundamental rights within the EU. Some examples can be found in some news articles online which bring up some of the challenges that come with the implementation of the EU AI Act:

The first example can be found in a news article from Epium Ltd., published in July 2025 and titled *"Swedish Prime Minister Urges Pause on EU's Artificial Intelligence Rules"*. The article discusses Ulf Kristersson, Sweden's Prime Minister, who is the first EU government leader to call for a halt to the implementation of the EU AI Act. In a meeting with Swedish Members of Parliament, he argues that the regulation is unclear, confusing and incomplete, especially regarding common technical standards, which may create problems if not clarified. He argues that these issues must be resolved before the regulation is implemented further. Kristersson also warns about the risk of Europe falling behind in AI systems, since some of them may not be available on the EU market under the current regulations. Some EU officials are now considering delaying the EU AI Act because the technical guidance needed to apply it may not be ready in time and that the law should be put on hold if key standards on things like cybersecurity and human oversight are still missing. Other officials from Poland, Sweden and the Czech Republic are among those who have expressed their concerns regarding this AI regulation.[170] The article illustrates several obstacles related to the EU AI Act due to it lacking clarity and then makes it confusing, that there are no common technical standards and this can later create problems in the European market as a result of losing access to some AI systems, as well as for cybersecurity and human oversight. These obstacles create significant challenges for the implementation of the EU AI Act and raise the question of whether some parts of the law should be postponed or revised in order to address the existing regulatory gaps.

A second example comes from a news article published in The Guardian in November 2025 titled *"Europe loosens reins on AI – and US takes them off"*. In this news piece, journalist Blake Montgomery discusses how the EU AI Act and the GDPR have been softened and postponed because Europe is increasingly viewed as losing ground to the US and China in innovation and AI technologies which also was a concern raised by Mario Draghi, one of Italy's former Prime Ministers. The article further explains that the European

[170] *See*, Epiqum, "Swedish Prime Minister Urges Pause on EU Artificial Intelligence Rules", published on 24 June 2025, available at epiqum.com/eu-ai-pause, accessed on 1 December 2025.

Commission is proposing a so-called *"digital omnibus"* package to simplify and align technology rules governing the EU AI Act, the GDPR, the ePrivacy Directive and the Data Act. It describes proposed changes to the GDPR that would loosen consent requirements for tech firms using individual's personal data to train AI systems and would reduce intrusive cookie banners, thereby making it easier for companies to use personal data. The Commission is also planning to delay the implementation of major parts of the EU AI Act, which has been in force since August 2024 but has not yet been fully applied to businesses.[171] This article underscores a significant obstacle for the EU AI Act due to certain provisions have already been delayed and this postponement may reflect an attempt by the EU to address its gap in AI-related innovation. In particular, it illustrates how the Act may be perceived as overly restrictive when compared with regulatory approaches in the US and China, and also how Article 7 of the GDPR could be undermined because the scope of an individual's right to give consent will be reduced.

Another example can be found in a newsletter written by Jessica Heesen and Tori Smith Ekstrand, published on The Conversation on 24 November 2025 under the title *"EU proposal to delay parts of its AI Act signal a policy shift that prioritises big tech over fairness"*. It addresses the pressure that has been placed on the EU by technology companies and the Trump administration regarding the implementation of the high-risk AI systems section of the EU AI Act. This has led the European Commission to propose changes to the EU AI Act and other data privacy regulations. At the same time, it has proposed delaying the implementation of the EU AI Act's key rules for high-risk AI systems, the ones that pose serious threats to individual's health, safety or fundamental rights, from the original period of August 2026–2027 to December 2027, with the possibility of further delays. The Commission claims these changes will help reduce the strain on European companies without undermining peoples rights or safety, but many critics see it as weakening the protection of ones rights and instead giving an advantage to major technology firms, particularly those based in the US.[172] This article highlights a key obstacle where the significant economic power that technology companies and certain politicians can influence on the EU AI Act. When policymakers within the EU or globally struggle to reach agreement with these AI technology companies, rules may be weakened or postponed. These delays, which can easily be extended, leave citizens less protected for longer periods and risk producing policies that prioritise business interests over people's fundamental rights.

---

[171] *See*, The Guardian, "Europe loosens reins on AI – and US takes them off", published on 25 November 2025, available at theguardian.com/us-europe-ai-rules, accessed on 1 December 2025.

[172] *See*, The Conversation, "EU proposal to delay parts of its AI Act signals a policy shift that prioritises big tech over fairness", published on 24 November 2025, available at theconversation.com/eu-ai-act-delay, accessed on 1 December 2025.

4.2 Balances of the US AI Regulation

The US Blueprint for an AI Bill of Rights and the NIST AI RMF 1.0 are two federal soft laws that set guidelines for how AI systems should be designed and used to protect the fundamental rights, freedoms and interests of individuals in the US. These soft law recommendations serve as non-binding federal policy documents and do not directly impose legal restrictions on AI systems within the US. Instead, they support and encourage US federal agencies, legislators and other policymakers in developing robust, rights-based AI regulations that help ensure the protection of individual rights, minimise biases and risks, and uphold transparency, accountability and sustainability.[173]

In other words, the NIST AI RMF 1.0 and the US Blueprint strive to reinforce and operationalise, rather than weaken, existing protections that complement rights already safeguarded under the U.S. Constitution, federal civil rights laws and other relevant federal legislation. In the US, most States, except for three, have either proposed or enacted some form of AI regulation at the state-level.[174] This demonstrates how these soft law instruments are decentralised and flexible, allowing all US States and federal bodies to choose whether and how to build upon these recommendations when deciding how to regulate AI within their jurisdictions, while maintaining and strengthening a fundamental rights framework at the federal policy level.

4.2.1 Fragmented Rights-Based AI Governance in the US: Federal Soft Law and State-Level Regulation

Although the US Blueprint for an AI Bill of Rights and the NIST AI RMF 1.0 establishing a federal soft law framework for rights-based AI governance, several obstacles hinder their effective implementation. Their non-binding nature, the highly decentralised regulatory landscape and the multiplication of varied state-level initiatives all hinder the achievement of coherent and consistent protection of fundamental rights across jurisdictions. Because US States and Federal Agencies may choose to bypass these soft law altogether or to adopt them only selectively, the frameworks capacity to meaningfully safeguard individual rights is weakened, even as AI technologies continue to be rapidly developed and deployed.[175] However, this does not prevent individual US States from adopting or strengthening their own AI regulations at the state-level. As a result, this may impose added obligations on AI-developing jurisdictions, such as California, Texas, New York, Illinois and others to implement forms of AI regulation that safeguard their residents, whereas, if it were adopted at the federal level, binding federal law would safeguard everyone in the US.

[173] AI Bill of Rights, *supra* note 45; National Institute of Standards and Technology, *supra* note 53.

[174] Bryan Cave Leighton Paisner LLP, *supra* note 55.

[175] Cox, *supra* note 56.

This approach risks building a patchwork of protections in which comparable AI systems are subject to divergent obligations depending on the state in which they are developed, deployed or used. Consequently, this kind of regulatory fragmentation can generate legal uncertainty for developers and regulated entities, make enforcement more difficult, and may lead to weaker consistency and effectiveness of rights-based AI governance at the federal level, where the NIST AI RMF 1.0 and the US Blueprint are not even taken into consideration.

4.3 Balances and Obstacles of China's AI Regulation

China's AI Governance Principles, the Deep Synthesis Provisions, and the Interim Measures for the Management of Generative AI Services combine elements of soft and hard law, forming an increasingly comprehensive framework for AI regulation. These instruments contain provisions on personal information protection, data security, transparency obligations and content labelling, which can, in practice, contribute to the protection of individual rights and interests. However, the fundamental structure of this regulatory framework is not grounded in a rights-based approach. Rather, it is primarily orientated towards maintaining social stability, safeguarding public order and national security, and ensuring that AI development and deployment remain under strong Government and Party oversight. In situations of conflict, collective and state interests are prioritised over individual claims, and rights-protective provisions are framed and interpreted through this broader lens of social and national security.[176]

While the existing AI regulatory frameworks in China seem to establish a balance between promoting the development of AI and implementing certain safeguards like the protection of personal data, data security obligations, transparency requirements and duties to label AI-generated content, this balance is fundamentally asymmetric. Individual rights are recognised, but they primarily operate as tools to achieve broader policy objectives (economic development, social stability, national security, etc.,) rather than as the central organising principle of AI governance. A range of systemic obstacles further limits the extent to which China's AI regulation can effectively protect individual rights in practice. Most significantly, the primary focus of the framework is security- and stability-oriented rather than rights-based. For example, in cases of conflict, collective and state interests are prioritised, and rights-based provisions are understood through prevailing narratives centred on social stability and national security.[177]

Moreover, the protection of rights is restricted by both administrative and regulatory limitations. There are few independent mechanisms for individuals to challenge AI-driven decisions, seek effective remedies or contest state and corporate uses of AI, especially in sensitive areas such as surveillance

[176] Gong, *supra* note 69; Huang et al., *supra* note 45, pp. 340–341.
[177] Huang et al., *supra* note 45, pp. 337 and 342–344.

and content management. Transparency and labelling requirements, while ostensibly rights-enhancing, also serve broader goals of information control and social management, further blurring the line between protection of peoples rights and control.[178] Taken as a whole, these structural features create significant obstacles to the effective protection and enforcement of individual rights in the context of AI in China.

4.3.1 AI-driven Rights Violations in China: A Landmark Court Case and Academic Report

China is a major player in the development of AI systems and already has some AI-related regulations, though publicly available information remains limited. These are explored below through a 2025 report and a 2024 court case. Taken together, they demonstrate that, in certain circumstances, individual plaintiffs can obtain remedies for AI-related rights violations, while also underscoring both the potential and the limits of rights-based protections, as well as the obstacles embedded in China's existing legal framework:

The first AI-related disputes emerged in a landmark case concerning AI-related voice rights. *Yin v. Baidu Netcom*, the Beijing Internet Court issued an April 2024 ruling addressing the protection of personal data and the incorporation of AI-driven voice imitation technologies by companies in their products.[179] The company's app operated an imitation service. Yin, the plaintiff, filed a lawsuit against the operators of the company's app, the AI software providers and the entrepreneurs because her voice was used in audiobooks without her consent and no contractual agreement was established with these entities. The AI applications that used her voice contributed to the platform's profits by replicating her voice. The court ruled that the defendants must pay Yin 1,214,400 yuan for breaching her data protection rights.[180] This case underscores the obligations that firms and AI developers in the economic and technological sectors must meet to ensure compliance with laws when using or making AI systems. All AI industries in China face the obstacle of striking a balance between protecting individual rights and fostering the advancement of AI technology. The companies and their AI systems can face penalties if they exploit or violate individual rights without obtaining consent or complying with Chinas regulations.

In December 2025, the Australian Strategic Policy Institute released an explanatory report covering the period from 2023 to 2025. Titled *"The party's AI: How China's new AI systems are reshaping human rights"*, it explains how the AI systems used in China's State Control are becoming more language model oriented and are being used to strengthen censorship, expand biometric surveillance and pre-empt opposition. The Chinese Communist

[178] Ibid, pp. 343–344.

[179] *See*, Beijing Internet Court, "BIC data rights circuit tribunal at ETDA holds 1st open hearing on data infringement case" (2024), available at bjinternetcourt.gov.cn/ai-copyright, accessed on 3 December 2025.

[180] *See*, Global Times, "Court rules on China's first AI voice rights case, sounding alarm for industry" (2024), available at globaltimes.cn/ai-governance, accessed on 3 December 2025.

Party introduced market incentives for private companies to develop AI technologies that are driven by censorship, which thereby reduces the costs and boosts the deployment. The report states that the growth of AI technology is giving China's state-backed companies more power over individuals in other countries and that many of the AI systems being sold abroad may contain some form of AI-enabled surveillance that can later lead to economic harm and unfair or biased treatment. These developments show how AI is increasingly being used to shape information, behaviour and economic outcomes in ways that heighten the risks of repression and human-rights abuses globally, while the report also offers evidence-based guidance on how to mitigate these harms.[181] The obstacles posed by AI systems used in this context can undermine individual rights such as freedom of expression, access to information and privacy. It enables mass tracking of individuals, monitoring and filtering of speech, and targeted repression that discourages free discussion and opposing viewpoints. They frequently depend on large-scale data collection and non-transparent AI systems that can encode and increase bias leading to discriminatory treatment and misidentification of ethnic minorities groups, as well as having economic consequences like for example loss of jobs or services based on flawed or biased AI decisions and usage.

[181] *See*, Australian Strategic Policy Institute, "The Party's AI: How China's New AI Systems Are Reshaping Human Rights" (2024), available at aspi.org.au/china-ai-human-rights, accessed on 3 December 2025.

Chapter 5

Conclusion and Policy Recommendations for Rights-Based AI Regulation

This dissertation has examined the role of a rights-based AI regulatory framework in protecting individual's fundamental rights. It employs comparative and doctrinal legal research to analyse AI legislation in the EU, the US, and China, focusing on how these jurisdictions protect fundamental rights within their AI regulatory frameworks. Through this analysis, it also explains the legal rules, government structure and political issues that make it difficult to put a human rights focused system of AI regulation into practice effectively.

5.1 Summary of Key Findings

Currently, there are very few, if any, AI-related legal cases or comprehensive regulations, because this is a rapidly developing and relatively new field. As a result, published research, policies and laws may change quickly. Each of the three jurisdictions has its own strategy, regulatory framework and approach to how AI systems are to be developed, deployed and used within its region. They can decide for themselves whether to adhere to the guidelines and standards set out in the OECD AI Principles, which aim to encourage the creation of innovative, safe and trustworthy AI systems worldwide. The dissertation reveals the following key findings to the main research questions:

The EU's AI Act is a hard law that places strong emphasis on developing trustworthy and sustainable AI systems that comply with the rights protections outlined in the EU Charter of Fundamental Rights, ECHR and to safeguard the integrity and stability of the Union. Protecting fundamental rights and ensuring trustworthy, sustainable AI are the central guiding principles behind how the EU designs and applies its AI regulations. All EU member states have until August 2027 to fully implement the EU AI Act and must establish competent authorities to monitor, supervise and enforce its implementation. In contrast, the US does not yet have a comprehensive federal AI regulation and its approach is more focused on innovation and competitiveness, supported by non-binding guidelines such as the AI Bill of Rights and the NIST AI Risk Management Framework which are soft laws.

These provide recommendations on how to safeguard people's rights, but implementation of these soft law recommendations is largely voluntary and may differ from state to state. Several states, including Texas, California, Colorado, Illinois and Hawaii, have already started enhancing their own AI regulations to prohibit the use of some AI systems in order to protect the rights of people who live in their state. China, however, has introduced a combination of AI-related soft laws and hard laws that prioritise state control, social stability and national security. While these laws make some reference to user protection, China's regulatory approach is more centred on preserving state interests and maintaining control over AI development and deployment than on protecting individual fundamental rights in the European sense. Overall, the EU aims to embed fundamental rights and trustworthy AI at the core of its binding regulatory framework, the US relies mainly on voluntary, innovation-driven guidance and fragmented state-level rules, and China emphasises state-centric objectives such as security and social stability, with comparatively less focus on individual rights. This demonstrates three different frameworks of AI governance, where there is a rights-based and trust-based framework in the EU, a innovation-driven and competitiveness-driven in the US, and a state control-oriented framework and security-oriented framework in China.

The EU AI Act seeks to balance AI development with the protection of people's fundamental rights by establishing a centralised, explicitly rights-based regulatory framework that builds in safeguards before AI systems are deployed. This regulation promotes more trustworthy, fair, safer, transparent and accountable AI, which helps minimise the risks of violating or negatively affecting fundamental rights. At the same time, several obstacles challenge this balance. Parts of the Act are unclear, which makes compliance confusing and may hinder effective implementation, and if EU countries do not share common technical standards for AI, the market may become fragmented. This can make some AI systems harder to access and weaken cybersecurity and human oversight. These regulatory gaps have triggered debates about postponing or revising some provisions, and delays already made signal that the EU is struggling to keep up with AI development while avoiding appearing more restrictive than the US or China. This situation could also affect data protection, as there are worries that individuals' consent rights may in practice be weakened. Another major obstacle is the economic and political power of large technology companies and certain politicians, who can shape both the content and timing of the rules. Difficult negotiations with these actors can produce weaker obligations or longer postponements, leaving EU citizens less protected. Ultimately, the balance between rights and innovation will depend on whether the EU can keep strong rights-based safeguards while managing innovation, standardisation and lobbying pressures without weakening fundamental rights protections.

In the US, rights-based AI regulation is partly balanced by soft law instruments like the NIST AI RMF 1.0 and the AI Bill of Rights Blueprint, which promote a fundamental rights framework at the federal policy level. Their decentralised and flexible nature allows federal agencies and US states to decide whether and how to adopt these recommendations. This kind of flexibility can promote experimentation and innovation in AI governance, while still pointing back to a shared rights-based framework. At the same time, it allows states like California, Texas, New York and Illinois to adopt or strengthen their own AI regulations that more directly safeguard their residents. However, the lack of binding federal AI legislation means that not everyone in the US has these rights-based protections. This creates a major obstacle and results in a fragmented set of protections, where similar AI systems can end up facing different requirements depending on whether they are being developed, deployed or used within a state. Such regulatory fragmentation in the US creates legal uncertainty for developers and regulated entities, which can lead to compliance and risk management difficulties. It also makes coordinated enforcement more difficult, particularly when AI systems cross state lines or operate on a national scale. The lack of mandatory federal consideration of the NIST AI RMF 1.0 and the US AI Bill of Rights Blueprint further undermines the consistency and effectiveness of rights-based AI governance. In general, the US strategy aims to balance flexibility and innovation with fundamental rights, but it faces significant challenges arising from decentralisation, legal fragmentation and inconsistent protections across state jurisdictions.

China's legal framework and case law on AI impose formal obligations on firms and developers to comply with rules on consent, data use and AI deployment, and to follow industry-specific standards and technical guidelines. These measures provide some regulatory balance and potential avenues for redress. However, rights-based AI regulation still faces significant obstacles because numerous AI systems in China enable mass surveillance, speech monitoring and targeted repression, weakening fundamental rights like freedom of expression, privacy and access to information. Large-scale data collection and non-transparent algorithms reinforce biases that can lead to discrimination, especially against ethnic minority groups and cause economic harms when flawed systems affect jobs, access to services, social benefits or financial opportunities. Moreover, AI's powerful role in social control, predictive governance and economic decision-making, combined with the prioritisation of national security and stability over individual rights, makes it difficult to fully ensure rights-based AI regulation in practice.

5.2 Recommendation for a Rights-Based AI Governance Framework

A EU rights-based AI governance framework should build on the EU AI Act, make fundamental rights protections legally binding and adaptable across all EU member states and be based on international human rights standards, thereby lowering the risks of violating the citizen's fundamental rights. In addition to this, the framework should clarify in detail how these protections apply to different types of AI systems, including general-purpose and foundation models, to prevent gaps and ensure consistent application across all sectors in the EU. Lawmakers should align the AI risk categories with rights impacts, develop shared risk classification systems and technical standards, along with creating international standards and certification frameworks for transparency, security and human oversight that are referenced across AI regulations, so that companies and public authorities can follow a clear set of standards when developing, deploying, and monitoring AI systems. High-risk AI systems should be subject to mandatory, harmonised fundamental rights impact assessments that directly address fundamental rights and human dignity, with special focus on vulnerable groups who may be unfairly affected, such as children, minorities or people in vulnerable employment situations. These assessments should be supported by compliance verification and additional obligations, including transparency responsibilities that make it easier for individuals to understand how the AI systems work, how they can raise complaints and how to resolve issues, for example by providing clear explanation when user interacts with an AI application, have public registers for certain high-risk AI systems and make it easy for people to complain, appeal or seek justice when companies or EU member states other than the one they live in violate their rights.

The US should establish federal regulations requiring AI technologies to comply with a rights-based standard and to meet similar criteria across all US jurisdictions, ensuring that fundamental protections do not depend on where a person happens to live or which agency governs the AI system. In other words, if an AI system is approved under one compliant framework, that approval should largely count towards meeting other similar frameworks, but the US states need to work together to reach this agreement through cooperative rule-making, mutual recognition arrangements and shared enforcement tools. At the same time, the federal level should set baseline rights protections that all US states or local governments are allowed to strengthen, but not weaken, thereby creating a progressive strengthening of rights protections while leaving room for innovation in governance. Interoperability initiatives must adhere to a non-regression principle that ensures existing rights cannot be weakened on the grounds of harmonisation, particularly in sensitive domains such as criminal justice, employment, housing, health care and access to public services. AI and data protection regulations must be aligned so that consent, purpose limitation and data minimisation are applied consistently, in both private-sector and public-sector uses, and so that individuals keep meaningful control over how their data is feed into AI technologies. Soft-law frameworks, such as risk-management frameworks, AI Bills of Rights and the NIST AI RMF 1.0 should correspond to a shared list of basic rights, receive formal legal acknowledgement and use consistent terminology, helping regulators, courts and AI developers to interpret obligations in a consistent and convergent manner.

China's governance rules should address institutional power imbalances by imposing stricter accountability, auditing and oversight duties on big tech companies and AI system providers, backed by strong, coordinated enforcement to prevent cross-border AI systems from exploiting regulatory gaps and undermining user protections. In light of the dangers of surveillance and repression, interoperable frameworks must incorporate explicit boundaries that prohibit AI applications which pose a threat to freedom of expression, privacy, equality, non-discrimination or access to information, including restrictions on mass biometric surveillance, social-scoring practices and profiling that targets political, religious or ethnic groups. Collaborative involvement by civil society, technical experts and affected communities should be ensured so that they can help review and revise AI regulations, which helps maintain their alignment with AI technological developments while safeguarding individual's fundamental rights and preventing the normalisation of invasive or discriminatory practices. Regular, transparent consultations, independent research public reporting obligations and mechanisms for reporting misconduct would further help reinforce a rights-based orientation which later can help enable a governance frameworks in China to develop in a progressive rights-based approach.

Overall, the EU, the US, and China should ground their AI regulations in a rights-based approach, ensuring that all individual rights at both the national and international levels are protected. The development and deployment of any AI technologies should be evaluated and regulated according to the level of risk it poses. Such a legal framework would help countries worldwide to trust each other's AI systems, thereby fostering more trustworthy AI technologies across jurisdictions without compromising rights protections and safety on a global scale.

5.3 Future Research Directions

Future studies on AI regulation in the EU, the US, and China should explore whether their regulatory models are moving toward interoperable frameworks that support trustworthy and sustainable AI or instead diverging into rival regulatory blocs. This entails examining mechanisms for dialogue, mutual learning, court and legal decisions, and collaborative risk governance, while also accounting for geopolitical frictions and differing constitutional principles. Such research may concentrate on analysing:

I. How different regulatory approaches shape compliance, innovation, transparency and accountability in AI technologies, with a particular focus on how non-state actors contribute to and influence AI governance. *a)* In the EU, industry bodies, civil society organisations and standards-setting institutions are central to implementation of the EU AI Act. *b)* In the US, large technology companies and self-regulatory schemes often fill gaps created by a decentralised federal state framework. *c)* In China, state-owned enterprises and industry associations translate broad policy goals into sector-specific rules under close government oversight.

II. How the AI regulations in each region impacts vulnerable groups, including racial and ethnic minorities, migrants, vulnerable workers and persons with disabilities. *a)* In the EU, it can involve testing whether the risk-based frameworks and fundamental rights impact assessments effectively prevent discrimination. *b)* In the US, the primary concern is how AI technology interacts with the civil rights law and inconsistent enforcement, particularly in policing, welfare, employment and credit. *c)* In China, the research can explore how large-scale data practices, social governance tools and public security systems shape the rights and everyday lives of vulnerable groups. A comparative study can help reveal how different constitutional and human-rights frameworks shape or limit rights-based regulation.

III. The relationship between AI technologies, Constitutional law and individual's fundamental rights. A comparative analysis of the three systems can help demonstrate how each structures AI governance and defines rights-based limits on governmental and corporate uses of AI technologies. *a)* In the EU, this relates to the Charter of Fundamental Rights, the European Convention on Human Rights and the legal systems of the EU member states. *b)* In the US, the research can focus on how the constitutional rights apply to algorithmic decision-making, surveillance and content moderation. *c)* In China, analysis can take into account a different constitutional and political framework, in which Party-state leadership, collective interests and social order shape both rights and restrictions on power.

Bibliography

Primary Sources

Legislation and Treaties

People's Republic of China

Constitution of the People's Republic of China (promulgated on 4 December 1982, amended in 2018).

Civil Code of the People's Republic of China (promulgated on 28 May 2020, effective on 1 January 2021).

Employment Promotion Law of the People's Republic of China (promulgated on 30 August 2007, effective on 1 January 2008).

Personal Information Protection Law of the People's Republic of China (promulgated on 20 August 2021, effective on 1 November 2021).

Provisions on the Management of Deep Synthesis for Internet Information Services (effective on 10 January 2023).

Interim Measures for the Management of Generative Artificial Intelligence Services (effective on 15 August 2023).

National New Generation Artificial Intelligence Governance Professional Committee, *Governance Principles for the New Generation Artificial Intelligence: Developing Responsible Artificial Intelligence* (2019).

European Union

Consolidated Version of the Treaty on European Union, 2012 O.J. (C 326) 13.

Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.

Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, 2000 O.J. (L 180) 22.

Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, 2000 O.J. (L 303) 16.

Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation, 2006 O.J. (L 204) 23.

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 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024 O.J. (L) (forthcoming).

European Commission, *Types of EU Law* (2024).

European Commission, *Equality Bodies* (2024).

European Commission, *Fundamental Rights Protection and Enforcement Under the AI Act* (2024).

International Instruments

International Convention on the Elimination of All Forms of Racial Discrimination, 21 December 1965, 660 U.N.T.S. 195.

International Covenant on Civil and Political Rights, 16 December 1966, 999 U.N.T.S. 171.

International Covenant on Economic, Social and Cultural Rights, 16 December 1966, 993 U.N.T.S. 3.

Office of the United Nations High Commissioner for Human Rights, *Status of Ratification Interactive Dashboard* (2025).

Organisation for Economic Co-operation and Development (OECD), *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (22 May 2019).

United Nations, *The 17 Sustainable Development Goals*, G.A. Res. 70/1 (21 October 2015).

Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/RES/217(III) (10 December 1948).

United States of America

Federal

U.S. Constitution's Amendments I–XXVII.

Civil Rights Act of 1964, Pub. L. No. 88-352, 78 Stat. 241 (codified as amended in scattered sections of 42, 28 U.S.C.).

Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 327 (codified as amended at 42 U.S.C. §§ 12101–12213).

The White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (October 2022).

U.S. Equal Employment Opportunity Commission, *Enforcement Guidance on Harassment in the Workplace* (29 September 2023).

State

California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199 (West 2020 & Supp. 2024).

California Privacy Rights Act of 2020, Cal. Civ. Code §§ 1798.100–1798.199.100 (effective on 1 January 2023).

Illinois Artificial Intelligence Video Interview Act, 820 Ill. Comp. Stat. 42/1–42/30 (2020).

New York City Automated Employment Decision Tools Law, N.Y.C. Admin. Code tit. 6, § 6-801 et seq. (effective on 5 July 2023).

Colorado Artificial Intelligence Act, Colo. Rev. Stat. §§ 6-1-1701 to 6-1-1706 (effective on 1 February 2026).

Texas Data Privacy and Security Act, Tex. Bus. & Com. Code Ann. §§ 541.001–541.155 (effective on 1 July 2024).

Hawaii Senate Bill 640, Relating to Artificial Intelligence, Haw. Rev. Stat. § 481B-4 (effective on 1 January 2025).

Case Law

Yin v Baidu Netcom, Beijing Internet Court (2024) (BIC Data Rights Circuit Tribunal at ETDA, 1st Open Hearing on Data Infringement Case).

Secondary Sources

Ajoodha, Thomas and Jared Browne, "Fundamental Rights Impact Assessments: What Are They? How Do They Work?", CEDPO AI and Data Working Group Micro-Insights Series (2025).

Amnesty International, "The Urgent but Difficult Task of Regulating Artificial Intelligence" (2024).

Australian Strategic Policy Institute, *The Party's AI: How China's New AI Systems Are Reshaping Human Rights* (2024).

Azam, Monirul, "Artificial Intelligence and EU Law: Risk, Sustainability and Public Good" in Katarina Claes and Christina Hioureas (eds), *AI and Fundamental Rights under the EU Law* (2019), pp. 85–119.

BBC News, "San Francisco is first US city to ban facial recognition" (14 May 2019).

Bryan Cave Leighton Paisner LLP, "US State-by-State Artificial Intelligence Legislation Snapshot" (2024).

Chae, Yoon, "U.S. AI Regulation Guide: Legislative Overview and Practical Considerations" (2020) 3(1) *RAIL: The Journal of Robotics, Artificial Intelligence & Law*, pp. 17–40.

Clark, Anna M and Paula P Plaza, "EU Artificial Intelligence Act: What Is It and How Does It Compare to U.S. AI Laws?" (2024).

Council of Europe, *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law* (2024).

Cox, Samantha, "Where AI Is Booming: Top U.S. States, Research Areas, and Industries" (2025).

Craig, Paul and Gráinne de Búrca, *EU Law: Text, Cases, and Materials* (8th edn, Oxford University Press 2024).

DagDok, *International Law - Conventions and Declarations* (2025).

DataGuard Insights, "The Growing Data Privacy Concerns with AI: What You Need to Know" (2024).

DLA Piper, "Data Protection Laws in the United States" (2025).

DLA Piper, "Europe: The EU AI Act’s Relationship with Data Protection Law: Key Takeaways" (2024).

Duane Morris LLP, "Illinois Enacts Artificial Intelligence Law Focused on Employment Practices" (2024).

Epiqum, "Swedish Prime Minister Urges Pause on EU Artificial Intelligence Rules" (24 June 2025).

Future of Life Institute, "Overview of all AI Act National Implementation Plans" (2024).

Global Times, "China Releases AI Governance Initiative, Advocates People-Centered Approach" (2024).

Global Times, "Court rules on China’s first AI voice rights case, sounding alarm for industry" (2024).

Gong, James, "What You Need to Know About China’s New Generative AI Measures" Bird & Bird (2023).

Huang, Xinbo et al, "The Legal Challenges and Regulatory Responses to Artificial Intelligence (AI) in China" in *Proceedings of the 12th UUM International Legal Conference 2023* (2024).

Levi, Stuart D et al, "Colorado’s Landmark AI Act: What Companies Need To Know" Skadden, Arps, Slate, Meagher & Flom LLP (2024).

National Institute of Standards and Technology, *AI Risk Management Framework* (2023).

Office of the Victorian Information Commissioner, *Artificial Intelligence and Privacy – Issues and Challenges* (2021).

Peczenik, Aleksander, "Empirical Foundations of Legal Dogmatics" (1969) 12(45) Logique et Analyse 31.

Pernot-Leplay, Emmanuel, "The AI Dilemma: AI Regulation in China, EU & the U.S." (2025).

Rodrigues, Rowena, "Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities" (2020) 4 Journal of Responsible Technology 100006.

Rubin, Tracy, Vince Sampson and Patrick Van Eecke, "Daily Journal Corporation: California's Bolstering Online Transparency Act targets bot disclosures in elections and transactions" (2024).

Salokannel, Pekka, "The Impact of AI: How Artificial Intelligence is Transforming Society" *3DBear Blog* (2023).

The Conversation, "EU proposal to delay parts of its AI Act signals a policy shift that prioritises big tech over fairness" (2025).

Tyman, Annette and Jason Priebe, "Artificial Intelligence Legal Roundup: Colorado Postpones Implementation of AI Law as California Finalizes New Employment Discrimination Regulations and Illinois Disclosure Law Set to Take Effect" Seyfarth Shaw LLP (2025).

Webster, Graham et al, "New Generation Artificial Intelligence Development Plan, State Council of China" (2017).