

Midwest Law Journal

Official Publication of the Midwest Academy of Legal Studies in Business

Volume XXXV

2025



Alice E. Keane, Carlos Ferran, Robert Garcia, <i>AI AND THE EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT: AN OVERVIEW</i> *Winner of the MLJ Best Article Award*	1
Wade S. Davis, Todd S. Lundquist, Katheryn L. Zielinski, <i>STRIPPING DOWN THE LAW: TEACHING WORKER CLASSIFICATION THROUGH EXOTIC DANCER LITIGATION</i>	30
Sameer Somal, William Choslovsky, <i>DECONSTRUCTING DEFAMATION DAMAGES: A THREE-RING LOOK AT REPUTATION</i>	69
John Paul, <i>HOMELESSNESS AND THE AMERICAN LEGAL ORDER: HISTORICAL FOUNDATIONS, COMPARATIVE PERSPECTIVES AND PATHWAYS TO REFORM</i>	91
Hershey H. Friedman, Robert B. Fireworker, <i>THE POWER OF ACTIVE LISTENING: A FOUNDATION FOR BUILDING TRUST, RESOLVING CONFLICT AND CULTIVATING UNDERSTANDING</i>	104

AI AND THE EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT: AN OVERVIEW

ALICE E. KEANE,* CARLOS FERRAN,** AND ROBERT GARCIA***

Artificial intelligence (“AI”) is transforming modern life. Its effects are being felt in nearly all areas of human endeavor, including art, medicine, education, employment, environmental protection, transportation, finance, crime fighting, and international conflicts.¹ Its growth, benefits, and harms are the subjects of innumerable news stories² and are only beginning to be understood as AI continues to develop at a rapid pace. Governments, businesses, and legal scholars worldwide are grappling with concerns about setting ethical and legal guardrails for this rapidly developing technology while balancing the importance of innovation.³ In a prescient move, the European Union spent roughly four years developing the first comprehensive AI law in the world, starting more than two years before AI exploded into the mainstream in November 2022 through the first widely available generative AI systems. On March 13, 2024, the European Parliament and the Council of the European Union approved the Artificial Intelligence Act (“EU AI Act” or “Act”).⁴ The Act uses a risk-based regulatory structure to ensure AI technology is transparent, safe, and aligned with fundamental human rights while working to maintain a competitive market for the digital economy. Through the EU AI Act, the European Union has set a precedent that is serving as a template for other jurisdictions in their attempts to regulate AI.

This article describes attempts to define AI, provides a history of its development, and discusses the reasoning for the need for AI regulation. It summarizes the EU AI Act, describing its risk-based regulatory framework, means of incentivizing AI development in safe places, AI sandboxes, and enforcement structure. For comparison, the status of AI law in the United States is examined at both the federal and state levels. The article then explores the future development of AI and the ability of the EU AI Act to address its growth.

* J.D., LL.M., Associate Professor of Accounting, Governors State University, Illinois.

** D.B.A., Ed.D., Professor of Accounting & Management Information Systems, Governors State University, Illinois.

*** Ph.D., Assistant Professor of Business Analytics & Management Information Systems, Governors State University, Illinois.

¹ Muhammad Tuhin, *The Pros and Cons of Artificial Intelligence*, SCI. NEWS TODAY, Apr. 23, 2025, <https://www.sciencenewstoday.org/the-pros-and-cons-of-artificial-intelligence/>.

² For a sampling of news stories covering AI, see, e.g., *Artificial Intelligence*, REUTERS, <https://www.reuters.com/technology/artificial-intelligence/>.

³ See, e.g., *Global AI Law and Policy Tracker*, IAPP, May 2025, <https://iapp.org/resources/article/global-ai-legislation-tracker/> (last visited Sept. 9, 2025); *AI Laws of the World: AI laws and proposed regulations across 40+ jurisdictions*, DLA PIPER, <https://intelligence.dlapiper.com/artificial-intelligence/>.

⁴ Renee Henson, *Bridging the Divide: Does the EU's AI Act Offer Code for Regulating Emergent Technologies in America*, 89 MO. L. REV. 847, 849 (Summer 2024); Sharon Klein & Lisa M. Campisi, *From Over the Pond: The European Union's Comprehensive AI Legislation Comes to America*, 54 THE BRIEF 22, 23 (American Bar Association) (Winter 2025). The EU AI Act was published in the EU's Official Journal on July 12, 2024. See Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, 2024 O.J. (L 202) 1, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (hereinafter “EU AI Act”).

I. BACKGROUND

A. WHAT IS AI?

Despite its widespread use, there is no agreed-upon definition of the term “artificial intelligence” or what specifically constitutes it.⁵ Part of the challenge with defining AI is that there is neither a formal definition of “intelligence” nor a theoretical basis for it that is not subjective.⁶ As computing devices grow in their ability to process vast amounts of data, the scientific community has sought a distinction between what is an actual intelligent system versus one that merely stores and retrieves data. In this sense, a distinction can be made between early views of intelligence as universal compression versus a more robust view of intelligence as the ability of comprehension.⁷

These distinctions on what an actual intelligent system is have led to a separation between what is termed strong and weak AI within the discipline.⁸ Some within the field maintain the goal of striving towards developing strong AI systems that mimic or surpass human capabilities of thought.⁹ While these goals of creating strong AI systems or even superintelligence have yet to be realized, progress towards them has led to many advancements within the field.

Among these advancements are Machine Learning (“ML”) algorithms that allow computers to learn from data and generate predictions or infer results.¹⁰ Research in ML is considered a subset of AI in which algorithms are designed around addressing domain-specific classes of problems.¹¹ Some of these, such as natural language processing and computer vision, among others, are believed to require some degree of intelligence.¹²

ML techniques attempt to realize this through a learning process where a machine is trained to recognize or learn patterns in data. The training can be done through supervised, unsupervised, and reinforcement learning approaches.¹³ Supervised approaches allow learning by example.¹⁴ In unsupervised approaches, an algorithm attempts to learn previously unknown patterns that exist within the data itself without relying on previous outcomes.¹⁵ Reinforcement learning uses a trial-

⁵ Christopher Collins, Denis Dennehy, Kieran Conboy & Patrick Mikalef, *Artificial Intelligence in Information Systems Research: A Systematic Literature Review and Research Agenda*, 60 INT’L J. INFO. MGMT. 102383, 2 (2021); LAURIE HARRIS, CONG. RESEARCH SERV., R48555, REGULATING ARTIFICIAL INTELLIGENCE: U.S. AND INTERNATIONAL APPROACHES AND CONSIDERATIONS FOR CONGRESS, R48555, at 1 (June 4, 2025).

⁶ BALAKRISHNAN CHANDRASEKARAN, *What Kind of Information Processing Is Intelligence?* in THE FOUNDATION OF ARTIFICIAL INTELLIGENCE—A SOURCEBOOK 14, 14 (Derek Partridge & Yorik Wilks eds., 1990).

⁷ José Hernández-Orallo & Neus Minaya-Collado, *A Formal Definition of Intelligence Based on an Intensional Variant of Algorithmic Complexity*, in PROC. INT’L SYMP. ENGINEERING INTELLIGENT SYS. (EIS98) (1998).

⁸ Paolo Bory, Simone Natale & Christian Katzenbach, *Strong and Weak AI Narratives: An Analytical Framework*, 40 AI & SOC’Y 2107, 2107 (2025).

⁹ DAVID J. GUNKEL, THE MACHINE QUESTION: CRITICAL PERSPECTIVES ON AI, ROBOTS, AND ETHICS 32 (MIT Press 2012).

¹⁰ GOPINATH REBALA, AJAY RAVI & SANJAY CHURIWALA, 2019 MACHINE LEARNING DEFINITION AND BASICS, AN INTRODUCTION TO MACHINE LEARNING 1, 2 (Springer 2019).

¹¹ *Id.*

¹² *Id.*

¹³ Niklas Kühl, Max Schemmer, Marc Goutier & Gerhard Satzger, *Artificial Intelligence and Machine Learning*, 32 ELECTRONIC MKTS. 2235, 2237-2238 (2022).

¹⁴ *Id.*

¹⁵ *Id.* at 2238.

and-error approach to perform actions that are rewarded to reinforce certain behavior.¹⁶ While each of these approaches is different, they all utilize some aspects of learning for their intelligence.

But learning methods are not the only aspects of intelligence that AI systems attempt to model. Some rule-based and expert system approaches attempt to mimic other aspects of intelligence. Unlike ML approaches, these algorithms can use inference or deductive reasoning for deriving answers. Other algorithms expand on what is learned. Evolutionary ML, for example, utilizes functions that mimic natural processes paired with ML to derive adaptive models that adjust to different conditions.¹⁷ Similarly, deep learning algorithms expand on existing learning algorithms by adding additional layers of abstraction, allowing the algorithms to understand more complex phenomena.¹⁸ However, like ML, these algorithms are limited to only specific intelligence functions.

Because of their limited intelligence capabilities and focus on specific classes of problems, these, along with ML, are often described as narrow or weak AI.¹⁹ Although the terms narrow or weak may imply a lesser role, these systems are currently the only realizable AI and have seen widespread use. Like the way research towards strong AI has informed ML in its early development, research on weak AI algorithms is being used to advance work towards strong AI.²⁰

Jory Schossau and Arend Hintze defined four stages towards realizing human cognition that expand upon strong and weak AI understandings; these include reactive machines, limited memory machines, theory of mind, and consciousness.²¹ Reactive machines include simple machines that take in input, process the input, and produce output.²² Limited memory machines, on the other hand, can retain and recall past information.²³ This is currently the limit of modern AI capabilities.²⁴ Expanding these abilities can form a theory of mind where the idea that others with different unexposed internal mental states exist, and a machine gains the ability to infer about these states. This can ultimately lead to consciousness or the realization of strong AI, where a machine acquires a sense of self-representation.²⁵

Whether they are reactive or limited memory, the current weak AI systems can perform a variety of different functions. Aside from ML, these also include machine vision, speech recognition, expert systems, robotics, and natural language processing.²⁶ Machine vision attempts to enable machines to analyze images, while speech recognition does the same for spoken words.²⁷ Expert systems attempt to simulate human problem-solving capabilities.²⁸ Robotics uses AI to generate

¹⁶ *Id.*

¹⁷ Akbar Telikani, Amirhessam Tahmassebi, Wolfgang Banzhaf & Amir H Gandomi, *Evolutionary Machine Learning: A Survey*, 54 ACM COMPUTING SURV. 1, 161:2 (2021).

¹⁸ Yann LeCun, Yoshua Bengio & Geoffrey Hinton, *Deep Learning*, 521 NATURE 436, 437 (2015).

¹⁹ HAROON SHEIKH, CORIEN PRINS & ERIK SCHRIJVERS, ARTIFICIAL INTELLIGENCE: DEFINITION AND BACKGROUND, MISSION AI: THE NEW SYSTEM TECHNOLOGY 15, 20 (Springer 2023).

²⁰ REBALA, *supra* note 10.

²¹ Jory Schossau & Arend Hintze, *Towards a Theory of Mind for Artificial Intelligence Agents*, in ARTIFICIAL LIFE CONF. PROC. 35, 21-22 (2023).

²² *Id.*

²³ *Id.*

²⁴ *Id.* at 21.

²⁵ *Id.* at 22.

²⁶ Collins, *supra* note 5, at 3.

²⁷ *Id.*

²⁸ *Id.*

computer-controlled motion of physical and virtual objects. Natural language processing allows a machine to process language.²⁹ However, modern AI systems are not limited to these functions. Many AI functions have been adapted to other problem areas, such as audio recognition and the recent paradigm shift of content creation through generative AI.³⁰

These varying AI functions and their adaptations have enabled AI to be used across different domains. The ways in which AI is used can vary. Ida Merete Enholm, Emmanouil Papagiannidis, Patrick Mikalef, and John Krogstie identify two broad categories of AI usage—automation and augmentation.³¹ For automation, AI is used for completing tasks typically done by humans, whereas for augmentation, it is used to aid in decision-making.³² A 2018 Harvard Business Review by Thomas Davenport and Rajeev Ronanki showed how AI was being used in projects to enhance business capabilities using process automation, cognitive insight, and cognitive engagement with employees and customers.³³ At the time, executives were benefiting from AI use in enhancing products and business capabilities. However, since then, with the release of ChatGPT in 2022, AI has seen widespread public adoption.³⁴ A survey by McKinsey & Company of 2,854 businesses across industries showed growth in usage from 55% in 2023 to 71% in 2024.³⁵ AI is already considered a disruptive technology in various sectors, including education, business, healthcare, agriculture, and urban development.³⁶ Yet, AI usage is continuing to grow in other areas as well, with the impact and types of usage varying by sector.³⁷

The complex inter-relationship between these different systems, technologies, and use domains is such that they are often discussed and viewed as if they were the same type of systems.³⁸ Further, the views of AI are often informed by myths, misrepresentations, and overestimations of its capabilities.³⁹ As AI becomes more mainstream, this lack of coherent AI understanding has raised concerns among researchers.⁴⁰ Aside from the need to define research avenues, questions have

²⁹ *Id.*

³⁰ Sandeep Singh Sengar, Affan Bin Hasan, Sanjay Kumar & Fiona Carroll, *Generative Artificial Intelligence: A Systematic Review and Applications*, MULTIMEDIA TOOLS & APPLICATIONS 23661, 23661-23662 (2024).

³¹ Ida Merete Enholm, Emmanouil Papagiannidis, Patrick Mikalef & John Krogstie, *Artificial Intelligence and Business Value: A Literature Review*, 24 INFO. SYS. FRONTIERS 1709, 1720 (2022).

³² *Id.*

³³ Thomas H. Davenport & Rajeev Ronanki, *Artificial Intelligence for the Real World*, 96 HARV. BUS. REV. 108, 110-112 (2018).

³⁴ Weixin Liang, Yaohui Zhang, Mihai Codreanu, Jiayu Wang, Hancheng Cao & James Zou, *The Widespread Adoption of Large Language Model-Assisted Writing Across Society*, arXiv:2502.09747, Feb. 19, 2025, <https://arxiv.org/abs/2502.09747>.

³⁵ Nestor Maslej, Loredana Fattorini, Raymond Perrault, Yolanda Gil, Vanessa Parli, Njenga Kariuki, Emily Capstick, Anka Reuel, Erik Brynjolfsson & John Etchemendy, ARTIFICIAL INTELLIGENCE INDEX REP. 2025, 261, arXiv:2504.07139 (Apr. 15, 2025).

³⁶ Vasile-Daniel Păvăloaia & Sabina-Cristiana Necula, *Artificial Intelligence as a Disruptive Technology—A Systematic Literature Review*, 12 ELECTRONICS 1102, 2 (2023).

³⁷ Shafeeq Ahmed Ali, Ali Ateeq, Marwan Milhem, Mohammed Alzoraik, Mohammed Abdulrazzaq Alaghbari & Baligh Beshr, *The Impact of Artificial Intelligence on Job Markets: A Sector-by-Sector Analysis*, in 2 BIG DATA IN FINANCE: TRANSFORMING THE FINANCIAL LANDSCAPE 457, 461 (Springer 2025).

³⁸ Kühl, *supra* note 13, at 2238.

³⁹ Sheikh, *supra* note 19, at 21–22; Savannah Thais, *Misrepresented Technological Solutions in Imagined Futures: The Origins and Dangers of AI Hype in the Research Community*, in AAAI/ACM CONF. AI, ETHICS, AND SOC’Y 1455 (2024).

⁴⁰ Dagmar Monett & Colin W.P. Lewis, *Getting Clarity by Defining Artificial Intelligence—A Survey*, in THIRD CONF. PHILOSOPHY & THEORY ARTIFICIAL INTELLIGENCE (2017).

been raised about what this lack of understanding could mean for AI policy.⁴¹ As industry leaders push the bounds of AI and its uses, there is an increasing interest in AI policy, laws, and governance.⁴² However, care must be taken to ensure that these are not informed by misrepresented views but instead by a realistic understanding of their capabilities and limitations.⁴³

To address these misunderstandings, there is a need for more work in clarifying AI narratives and understanding.⁴⁴ In its simplest view, AI is really just the automation of cognition. As discussed, this automation can be complicated in that it can take on many different forms based on the level of cognition, functions, and has many different domains of usage. While the scientific community continues to expand on understandings of AI, government entities like the European Union Commission (“Commission”) are working to define AI.⁴⁵ According to the Commission:

Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal.⁴⁶

The Organization for Economic Cooperation and Development (“OECD”) also incorporated a definition of AI in its OECD AI Principles, which states:

An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.⁴⁷

The AI Principles have been adopted by forty-seven countries as of May 2025, including the United States and the European Union.⁴⁸

⁴¹ Sabkalp Bhatnagar, Anna Alexandrova, Shahar Avin, Stephen Cave, Lucy Cheke, Matthew Crosby, Jan Feyereisl, Marta Halina, Bao Sheng Loe & Seán Ó hÉigeartaigh, *Mapping Intelligence: Requirements and Possibilities*, in THIRD CONF. PHILOSOPHY & THEORY ARTIFICIAL INTELLIGENCE 117, 119 (2017).

⁴² Huw Roberts, Emmie Hine, Mariarosaria Taddeo & Luciano Floridi, *Global AI Governance: Barriers and Pathways Forward*, 100 INT’L AFF. 1275, 1275 (2024).

⁴³ Thais, *supra* note 39, 1455.

⁴⁴ Bory, *supra* note 8, at 2107–08.

⁴⁵ Hleg Ai, *High-Level Expert Group on Artificial Intelligence*, in ETHICS GUIDELINES FOR TRUSTWORTHY AI 1 (2019).

⁴⁶ *Id.* at 6.

⁴⁷ Organisation for Economic Co-operation and Development [OECD], *Explanatory Memorandum on the Updated OECD Definition of an AI System*, OECD Artificial Intelligence Papers No. 8 (Mar. 2024) https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/03/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_3c815e51/623da898-en.pdf.

⁴⁸ Organisation for Economic Co-operation and Development [OECD], *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (May 22, 2019; amended Mar. 5, 2024) <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>.

While these definitions provide a good overview of the current state of AI understanding, it is likely that ideas of what AI is will continue to evolve with AI. To examine this further, it is important to understand the development of AI and its history.

B. THE DEVELOPMENT OF AI

The history of AI represents a complex trajectory of conceptual breakthroughs, technical advances, and periods of recalibration, punctuated by shifting societal and regulatory currents. While the ambition to create thinking machines is ancient, the scientific journey began in the mid-20th century with the convergence of mathematics, logic, and early computing theories. This evolution from symbolic reasoning to data-driven learning systems ultimately necessitated comprehensive regulatory frameworks like the EU AI Act.

1. FOUNDATIONAL PERIOD AND EARLY AI (1940s–1980s)

The mathematical groundwork emerged from Warren S. McCulloch and Walter Pitts⁴⁹ who introduced artificial neural networks and established foundations for understanding the brain as a computational system. Alan Turing’s landmark paper “Computing Machinery and Intelligence” introduced the “Imitation Game” (now the Turing Test), framing the fundamental question “Can machines think?” and providing a measure for machine intelligence.⁵⁰ Turing had conceptualized ML during World War II, envisioning computers that could “learn from experience” and modify their own instructions.⁵¹

The formal genesis of AI as a field is attributed to the 1956 Dartmouth Summer Research Project on Artificial Intelligence, where John McCarthy coined the term “artificial intelligence.”⁵² The workshop united researchers who believed that “every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to make it.”⁵³ This era was dominated by “Good Old-Fashioned AI” (GOFAI) or symbolic AI, which posited that intelligence could be replicated by manipulating symbols according to formal rules.⁵⁴

Early breakthroughs included Allen Newell and Herbert A. Simon’s Logic Theorist, capable of proving mathematical theorems, and the development of the first artificial neural network, SNARC (Stochastic Neural Analog Reinforcement Calculator), by Marvin Minsky and Dean Edmonds in 1951.⁵⁵ John McCarthy’s development of LISP in 1958 became a standard programming language

⁴⁹ Warren S. McCulloch & Walter Pitts, *A Logical Calculus of The Ideas Immanent in Nervous Activity*, BULL. MATHEMATICAL BIOPHYSICS 5(4), 115–133 (1943).

⁵⁰ Alan M. Turing, *Computing Machinery and Intelligence*, MIND 49(236), 433–460 (1950).

⁵¹ Alan M. Turing, *Lecture to the London Mathematical Society on 20 February 1947*, CHARLES BABBAGE INST. REPRINT SERIES HIST. COMPUTING 10 (1947).

⁵² John McCarthy, Marvin Minsky, Nathaniel Rochester & Claude Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, AI MAG., 27(4), 12–14 (reprint of 1955 proposal) (2006).

⁵³ *Id.*

⁵⁴ JOHN HAUGELAND, *ARTIFICIAL INTELLIGENCE: THE VERY IDEA* (MIT Press 1985).

⁵⁵ Allen Newell & Herbert A. Simon, *The Logic Theory Machine—A Complex Information Processing System*, IRE TRANSACTIONS ON INFORMATION THEORY, 2(3), 61–79 (1956); Marvin L. Minsky, *Theory of Neural-Analog Reinforcement Systems and Its Application to the Brain-Model Problem* (1954) (Ph.D. dissertation, Princeton University) https://people.csail.mit.edu/brooks/idocs/Marvin_Minsky_PhD_Princeton_1953_1954.pdf.

for AI research, providing powerful tools for symbolic processing.⁵⁶ Concurrently, Arthur Samuel developed the world’s first self-learning program for checkers and coined the term “machine learning.”⁵⁷

The 1960s witnessed the creation of ELIZA, the first chatbot by Joseph Weizenbaum, which used natural language processing to simulate conversation.⁵⁸ This early system provided a prescient glimpse of human-machine interaction challenges that would later inform the EU AI Act’s provisions on AI systems that interact with natural persons, particularly regarding transparency obligations and the requirement to inform users when they are interacting with an AI system.⁵⁹ Another key development was Shakey the robot at Stanford Research Institute, the first mobile intelligent robot combining AI, computer vision, and navigation.⁶⁰

However, initial exuberance encountered significant challenges. Marvin Minsky and Seymour A. Papert’s *Perceptrons* highlighted limitations of simple neural networks, leading to reduced interest.⁶¹ Combined with insufficient computational power, limited data, and the immense difficulty of encoding common-sense knowledge, a period of reduced funding known as the first “AI winter” began, exacerbated by James Lighthill’s critical 1973 report that led to significant funding reductions.⁶²

2. THE AI RENAISSANCE AND THE RISE OF ML (1980s–2016)

The 1980s marked an AI renaissance with the commercialization of expert systems, driven by a paradigm shift from symbolic reasoning to ML, where systems learn patterns from data without explicit programming. The increasing availability of large datasets, advances in computing power, and new technical developments enabled this transformation.

The development of backpropagation algorithms gained prominence through David E. Rumelhart, Geoffrey Hinton, and Ronald J. Williams’ influential paper “Learning representations by back-propagating errors,” which enabled the training of multilayer neural networks and reinvigorated research interest.⁶³ John Hopfield’s proof that certain neural networks could learn and process information further advanced the field.⁶⁴ The shift toward mathematically rigorous

⁵⁶ John McCarthy, *Recursive Functions of Symbolic Expressions and Their Computation by Machine, Part I*, COMM. ACM, 3(4), 184–195 (1960).

⁵⁷ Arthur L. Samuel, *Some Studies in ML Using the Game of Checkers*, IBM J. RES. DEV., 3(3), 210–229 (1959).

⁵⁸ Joseph Weizenbaum, *ELIZA—A Computer Program for the Study of Natural Language Communication Between Man and Machine*, COMM. ACM, 9(1), 36–45 (1966).

⁵⁹ *Id.* at 36–45; EU AI Act, *supra* note 4.

⁶⁰ Nils J. Nilsson, *Shakey the Robot, Technical Note 323*, SRI INT’L, April 1984, <https://ai.stanford.edu/~nilsson/OnlinePubs-Nils/shakey-the-robot.pdf>.

⁶¹ MARVIN MINSKY & SEYMOUR A. PAPERT, *PERCEPTRONS: AN INTRODUCTION TO COMPUTATIONAL GEOMETRY* (MIT Press 1969).

⁶² James Lighthill, *Artificial Intelligence: A General Survey*, SCI. RES. COUNCIL, July 1973, https://rodsmith.nz/wp-content/uploads/Lighthill_1973_Report.pdf.

⁶³ David E. Rumelhart, Geoffrey E. Hinton & Ronald J. Williams, *Learning Representations by Back-Propagating Errors*, NATURE 323(6088), 533–536 (1986).

⁶⁴ John J. Hopfield, *Neural Networks and Physical Systems with Emergent Collective Computational Abilities*, PROC. NAT’L ACAD. SCI. 79(8), 2554–2558 (1982).

approaches continued with Judea Pearl’s work on probabilistic reasoning⁶⁵ and Lotfi Zadeh’s (1965) fuzzy logic systems.⁶⁶

The 1990s witnessed major practical breakthroughs. IBM’s statistical approach to machine translation in 1990 marked a pivotal shift from rule-based to probabilistic methods in natural language processing.⁶⁷ The defeat of chess champion Garry Kasparov by IBM’s Deep Blue in 1997 demonstrated the power of specialized, data-driven AI.⁶⁸

The modern era of AI was launched by Geoffrey Hinton’s 2006 publication of techniques for training deep neural networks,⁶⁹ enhanced by innovations in GPU computing.⁷⁰ The true inflection point arrived with the 2012 ImageNet competition, where AlexNet dramatically outperformed all other methods in image recognition, launching the current “AI spring.”⁷¹ This breakthrough unlocked unprecedented computer vision, speech recognition, and natural language processing capabilities, moving AI from the laboratory to mainstream applications.⁷²

This period of explosive growth directly created the technological conditions for deep learning technologies in critical domains:

- Biometric identification systems: The power of deep learning in facial recognition and real-time remote biometric identification led to its widespread use in surveillance, raising fundamental rights concerns.⁷³
- Algorithmic bias and discrimination: ML models trained on historical data began replicating and amplifying existing societal biases, leading to high-profile cases of discrimination in criminal justice risk assessment, hiring algorithms, and credit scoring.⁷⁴
- Lack of transparency and explainability: The complexity of deep learning models, often termed “black boxes,” made it difficult to understand their decision-making processes. This opacity became a central challenge, directly informing the development of explainable AI (“XAI”) as both a technical field and regulatory necessity.⁷⁵

⁶⁵ JUDEA PEARL, *PROBABILISTIC REASONING IN INTELLIGENT SYSTEMS: NETWORKS OF PLAUSIBLE INFERENCE* (Morgan Kaufmann ed., 1988).

⁶⁶ L.A. Zadeh, *Fuzzy sets*, INFO. CONTROL 8(3), 338–353 (1965).

⁶⁷ Peter F. Brown, et al., *A Statistical Approach to Machine Translation*, COMPUTATIONAL LINGUISTICS 16(2), 79–85 (1990).

⁶⁸ FENG-HSIUNG HSU, *BEHIND DEEP BLUE: BUILDING THE COMPUTER THAT DEFEATED THE WORLD CHESS CHAMPION* (Princeton University Press 2002).

⁶⁹ Geoffrey E. Hinton, Simon Osindero & Y.W. Teh, *A Fast Learning Algorithm for Deep Belief Nets*, NEURAL COMPUTATION 18(7), 1527–1554 (2006).

⁷⁰ Rajat Raina, Anand Madhavan & Andrew Y. Ng, *Large-Scale Deep Unsupervised Learning Using Graphics Processors*, PROC. 26TH ANN. INT’L CONF. MACHINE LEARNING 873–880 (2009).

⁷¹ Alex Krizhevsky, Ilya Sutskever & Geoffrey E. Hinton, *Imagenet Classification with Deep Convolutional Neural Networks*, ADVANCES NEURAL INFO. PROCESSING SYS. 25 (2012).

⁷² IAN GOODFELLOW, YOSHUA BENGIO & AARON COURVILLE, *DEEP LEARNING* (MIT Press 2016).

⁷³ EU AI Act, *supra* note 4.

⁷⁴ Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, PROPUBLICA, May 23, 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

⁷⁵ Amina Adadi & Mohammed Berrada, *Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)*, 6 IEEE ACCESS 52138, Sept. 17, 2018, <https://ieeexplore.ieee.org/document/8466590>.

3. THE GENERATIVE AI BOOM AND REGULATORY ADAPTATION (2017–PRESENT)

The most profound recent shift has been the rise of generative AI, particularly Large Language Models (“LLMs”). The development of the Transformer architecture in “Attention Is All You Need”⁷⁶ was pivotal. Based on attention mechanisms, it enabled parallel processing and significantly improved the modeling of long-range dependencies, spawning major model lines like Google’s BERT and OpenAI’s GPT.⁷⁷

ChatGPT’s public release in November 2022 marked a significant turning point, demonstrating generative AI’s power to a global audience and reaching 100 million users within two months.⁷⁸ These models could generate coherent text, write code, and engage in complex conversation, showcasing their potential as general-purpose AI (“GPAI”) models with wide-ranging capabilities.⁷⁹ GPT-4’s release in March 2023 demonstrated even more sophisticated reasoning and multimodal understanding.⁸⁰

Since 2022, the pace of AI development has accelerated rather than slowed. The global AI market reached \$638.23 billion in 2024 and is projected to reach \$3,680.47 billion by 2034, highlighting the continued economic significance of AI technologies.⁸¹ Business adoption has accelerated, with 78 percent of organizations using AI in at least one function.⁸²

The development of AI from its mathematical foundations in the 1940s to today’s sophisticated LLMs represents one of the most significant technological transformations in human history. The journey from simple neural networks to transformer-based systems capable of human-like reasoning has been marked by periods of optimism, disappointment, and breakthrough innovation. As AI systems have become increasingly powerful and pervasive, the concurrent development of comprehensive regulatory frameworks demonstrates the critical importance of balancing innovation with safety, transparency, and respect for fundamental rights.

C. WHY REGULATE AI?

AI is capable of providing enormous benefits for humanity in a growing variety of areas of human endeavor, including environmental protection, food scarcity and poverty alleviation, healthcare, accessibility and accommodation for people with disabilities, employment, education,

⁷⁶ Ashish Vaswani, A., et al., *Attention is all you need*, ADVANCES NEURAL INFO. PROCESSING SYS. 30 (Dec. 4, 2017).

⁷⁷ Jacob Devlin, Ming-Wei Chang, Kenton Lee & Kristina Toutanova, *BERT: Pre-Training of Deep Bidirectional Transformers for Language Understanding*, ARXIV, May 24, 2019, <https://doi.org/10.48550/arXiv.1810.04805>; Alec Radford, Karthik Narasimhan, Tim Salimans & Ilya Sutskever, *Improving Language Understanding by Generative Pre-Training*, OPENAI (2018) https://cdn.openai.com/research-covers/language-unsupervised/language_understanding_paper.pdf.

⁷⁸ OPENAI, INTRODUCING CHATGPT (Nov. 30, 2022) <https://openai.com/blog/chatgpt>.

⁷⁹ *Id.*

⁸⁰ OpenAI, *GPT-4 Technical Report*, ARXIV, Mar 27, 2023, <https://doi.org/10.48550/arXiv.2303.08774>.

⁸¹ Aarti Dhapte, *Global Artificial Intelligence Market Research Report*, MKT. RES. FUTURE, Sept. 2025, <https://www.marketresearchfuture.com/reports/artificial-intelligence-market-1139>.

⁸² McKinsey & Company, *The state of AI in early 2024: Gen AI Adoption Spikes and Starts to Generate Value*, May 30, 2024, <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024>; McKinsey & Company, *The State of AI: How Organizations are Rewiring to Capture Value*, Mar. 12, 2025, <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>.

transportation, and law enforcement.⁸³ For example, AI is already being used to assist doctors in diagnosing diseases, predicting patient outcomes, and personalizing treatments.⁸⁴ It can also improve access to educational resources and offer personalized tutoring, preserve and teach endangered languages, significantly improve the efficiency of computer programming, and accelerate breakthroughs in science.⁸⁵ In addition, AI is important in helping maintain national and global security.⁸⁶

However, AI also has the potential to cause serious harm, either intentionally or unintentionally.⁸⁷ The parade of horrors listed as reasons for its regulation is long. For example, through the use of fake news and deep fakes, AI has the potential to ““endanger lives, fair elections and the course of history.””⁸⁸ It “can be used to fool security systems and people,” “mislead voters, spread false information about people, or sway public opinion.”⁸⁹ It can covertly manipulate consumer behavior, and the use of “biometric data may permit one to infer a person’s thoughts, intentions, emotions, or stress levels.”⁹⁰ Bias in AI systems can negatively impact certain groups in lending, employment, and admissions to universities.⁹¹ It can exacerbate income disparities and poverty, cybercrime, and climate change.⁹² And it poses serious risks to public safety, including being used to develop weapons and commit widespread fraud and other crimes.⁹³

Given the breadth of benefits and harms possible, scholars have asked how governments can promote the benefits of AI while limiting its potential for harm.⁹⁴ Two approaches to regulating AI and technology have been proposed—a “rights-based approach,” which focuses on providing rights to individuals, like privacy and freedom of expression, and a “risk-based approach,” which focuses on reducing harm by regulating AI depending on the risk that it poses to human rights and safety.⁹⁵ The EU AI Act takes a risk-based approach and attempts to limit harm through its risk-

⁸³ See Orly Lobel, *The Law of AI for Good*, 75 FLA. L. REV. 1073, 1094-1108 (2023); Keith E. Sonderling, Bradford J. Kelley & Lance Casimir, *The Promise and The Peril: Artificial Intelligence and Employment Discrimination*, 77 U. MIAMI L. REV. 1, 5 (Fall 2022).

⁸⁴ Hamsa Hassan & Hussain Aldawood, *Ensuring Data Protection, Security and AI Ethics in AI Systems*, PRIVACY DATA PROTECTION 25 (12) (Dec. 1, 2024).

⁸⁵ Maroussia Lévesque, *Smoke and Mirrors? Corporate Discretion in AI Regulation*, 2025 U. ILL. J.L. TECH. & POL’Y 33, 44 (Spring 2025).

⁸⁶ Steven Arango, *A Legislative Foundation for Foundation Models*, 41 GA. ST. U.L. REV. 531, 547 (Spring 2025), citing COMM’N ON A.I. COMPETITIVENESS, INCLUSION & INNOVATION, U.S. CHAMBER OF COMM., REPORT AND RECOMMENDATIONS 63 (2022).

⁸⁷ Stephen T. Black, *Weaponizing AI*, 16 HASTINGS SCI. & TECH. L.J. 117 (April 2025).

⁸⁸ *Id.* at 186, quoting The University of Queensland, *How AI Is Being Used to Fight Fake News*, CHRON. HIGHER EDUC. (2020), <https://sponsored.chronicle.com/how-ai-is-being-used-to-fight-fake-news/index.html>.

⁸⁹ Black, *supra* note 87, at 189-190.

⁹⁰ Henson, *supra* note 4, at 852-853.

⁹¹ Black, *supra* note 87, at 192; Sonderling, *supra* note 83, at 6-9; Natalie Sheard, *No Notice and No Explanation: The Incontestability of Hiring Discrimination by Algorithm*, 35 AUSTL. J. LABOUR L. 119 (Nov. 2022); see generally *Chapter One: Resetting Antidiscrimination Law in the Age of AI*, 138 HARV. L. REV. 1562 (April 10, 2025).

⁹² Josephine Wolff, William Lehr, & Christopher S. Yoo, *Lessons from GDPR for AI Policymaking*, 27 VA. J.L. & TECH. 1, 6 (Winter 2024).

⁹³ Lobel, *supra* note 83, at 1077-1078.

⁹⁴ Black, *supra* note 87, at 203; Lobel, *supra* note 83, at 1073.

⁹⁵ Daniel Leufer & Fanny Hidvegi, *The Pitfalls of the European Union’s Risk-Based Approach to Digital Rulemaking*, 71 UCLA L. REV. DISC. 156, 159-160 (May 21, 2024).

based structure of regulation, while allowing low-risk and no-risk AI systems to be developed with limited or no regulatory oversight.⁹⁶

II. WHAT THE EU AI ACT DOES

The EU AI Act is the most comprehensive AI law in the world.⁹⁷ It joins other regulations in the European Union in regulating technology and protecting fundamental human rights, privacy, and data, including the General Data Protection Regulation (“GDPR”),⁹⁸ the European Convention on Human Rights,⁹⁹ and the EU Charter.¹⁰⁰

The European Union took a risk-based approach in developing the EU AI Act, rather than a rights-based approach; thus, it is focused on regulating owners and operators of AI systems based on their risks rather than on providing individuals with rights to data protection, for instance.¹⁰¹ The Act regulates all types of AI based on each type’s risk to humans, rather than by attempting to predict how AI will grow and change.¹⁰² In this way, the EU AI Act provides “a holistic risk-based regulatory framework,”¹⁰³ rather than regulating types or sectors of AI specifically.

The purpose of the EU AI Act

is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, [and] fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation.¹⁰⁴

The potential harms that the Act is designed to prevent include “creating disinformation, displacing workers, and harming national security,”¹⁰⁵ generating disinformation, cyberweapons, bioweapons, spearphishing emails, creating malware, committing financial fraud, and generating and disseminating child pornography.¹⁰⁶

⁹⁶ *Id.* at 166-167.

⁹⁷ Lévesque, *supra* note 85, at 105.

⁹⁸ EU AI Act, *supra* note 4.

⁹⁹ Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, Europ. T.S. No. 5, 213 U.N.T.S. 221.

¹⁰⁰ Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391. For an analysis of these laws and their impact on privacy data protection, see Olga Kokoulina, *Towards Future-Proof, Rights-Respecting Automated Data Collection: An Examination of European Jurisprudence*, 26 VAND. J. ENT. & TECH. L. 707, 732-745 (Summer 2024); Iain Nash, DeBrae Kennedy-Mayo, Peter Swire & Annie Antón, *Legal Issues in Reconciling Data Protection, AI, and Cybersecurity under EU Law*, 89 MO. L. REV. 871, 884-903 (Summer 2024).

¹⁰¹ Wolff, *supra* note 92, at 20; Daniel J. Solove & Woodrow Hartzog, *Kafka in the Age of AI and the Futility of Privacy as Control*, 104 B.U.L. REV. 1021, 1040 (2024).

¹⁰² Pablo A. Iannello, *Trust But Verify ... As Long as You Can. Transparency, Consent Management and Their Limits in a Big Data-Machine Learning Environment*, 50 DAYTON L. REV. 329, 337; see *infra* Table 1: Risks explicitly regulated by the EU AI Act.

¹⁰³ Arango, *supra* note 86, at 545.

¹⁰⁴ EU AI Act, *supra* note 4, art. 1, 1.

¹⁰⁵ Arango, *supra* note 86, at 534.

¹⁰⁶ *Id.* at 542-543.

The EU AI Act has been described as “a four-tiered structure [that] bars systems with unacceptably high-risk, closely tracks high-risk systems, requires basic transparency for limited risk deployments, and encourages voluntary codes of conduct for minimally risky systems.”¹⁰⁷

In the EU AI Act, “AI system” is defined as

a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.¹⁰⁸

The Act applies to all AI providers, deployers, importers, distributors, and product manufacturers whose AI systems are used within the European Union, authorized representatives of providers not established within the European Union, and affected persons located in the European Union.¹⁰⁹ Because of the extraterritoriality of the Act, its “broad scope will reverberate throughout other countries.”¹¹⁰

The Act contains specific exclusions from regulation. It expressly does not apply to AI systems that are put into service or used exclusively for military, defense, or national security purposes.¹¹¹ It does not apply to natural persons using AI systems in purely personal, non-professional activities or free and open-source AI systems.¹¹² Finally, it does not apply to research, testing, or development of AI systems or models before they are placed on the market or put into service, though research, testing, or development in real-world conditions within the European Union is regulated by the Act.¹¹³ Such research, testing, or development takes place in design spaces called “AI sandboxes” set up by member states and others.¹¹⁴

The Act categorizes AI systems based on risk level, where “risk” is defined as “the combination of the probability of an occurrence of harm and the severity of that harm.”¹¹⁵ AI systems are divided into risk categories, which are regulated differently: (1) unacceptable risk AI systems¹¹⁶; (2) high-risk AI systems¹¹⁷; and (3) GPAI systems, which may be determined to have systemic risk or not.¹¹⁸

A. UNACCEPTABLE RISK AI SYSTEMS

Certain highly risky AI systems are prohibited under the Act.¹¹⁹ The Act bans putting into service AI systems that:

¹⁰⁷ Lévesque, *supra* note 85, at 48.

¹⁰⁸ EU AI Act, *supra* note 4, art. 3, (1).

¹⁰⁹ *Id.* art. 2(1)(a)-(g).

¹¹⁰ Henson, *supra* note 4, at 851.

¹¹¹ EU AI Act, *supra* note 4, at art. 1, 3.

¹¹² *Id.* art. 1(10), (12).

¹¹³ *Id.* art. 1(8).

¹¹⁴ *Id.* art. 3(55).

¹¹⁵ *Id.* art. 3(2).

¹¹⁶ *Id.* art. 5.

¹¹⁷ *Id.* art. 6-27.

¹¹⁸ *Id.* art. 51-56.

¹¹⁹ *Id.* art. 5.

- deploy subliminal or purposefully manipulative or deceptive techniques¹²⁰;
- exploit users because of their age, disability, or social or economic situation¹²¹;
- evaluate or classify natural persons or groups based on social behavior or known, inferred, or predicted personal or personality characteristics leading to detrimental or unfavorable treatment of natural persons or groups¹²²;
- make risk assessments of natural persons to predict criminal behavior based on profiling or assessing personality traits and characteristics (not applicable to AI systems supporting human assessment of involvement of a person in criminal activity that is already based on objective and verifiable facts directly linked to criminal acts)¹²³;
- create or expand facial recognition databases through untargeted scraping from the internet or CCTV sources¹²⁴;
- infer emotions of natural persons in the workplace or educational institutions except for medical or safety reasons¹²⁵;
- categorize natural persons based on biometric data to deduce “race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation”¹²⁶;
- use real-time remote biometric identification systems in public areas for law enforcement, except as strictly necessary for
 - searches for victims of abduction, trafficking, sexual exploitation, or missing persons,
 - prevention of specific, substantial, and imminent threat to natural persons or genuine present or foreseeable threat of terrorist attack,
 - location or identification of specific suspects for serious crimes.¹²⁷

Noncompliance with the prohibitions in the EU AI Act on unacceptable risk systems is punished severely. It can result in fines of up to €35 million or up to 7 percent of a provider’s annual worldwide turnover for the preceding financial year, whichever is higher.¹²⁸

B. HIGH-RISK AI SYSTEMS

Certain AI systems are designated as high-risk in the EU AI Act based on their uses. These include AI systems used in:

- remote biometric identification, biometric categorization, and emotion recognition;
- safety components in digital infrastructure, road traffic, or supply of water, gas, heating, or electricity;
- education and vocational training admissions, learning outcomes, and other uses;
- employment, workers’ management, and access to self-employment;
- access to essential private and public services and benefits, including healthcare, credit scoring, life and health insurance, and dispatching of emergency first responders;

¹²⁰ *Id.* art. 5(1)(a).

¹²¹ *Id.* art. 5(1)(b),

¹²² *Id.* art. 5(1)(c).

¹²³ *Id.* art. 5(1)(d). The list of criminal behavior covered is included in annex II of the AI Act. *Id.* annex II.

¹²⁴ *Id.* art. 5(1)(e).

¹²⁵ *Id.* art. 5, 1(f).

¹²⁶ *Id.* art. 5, 1(g).

¹²⁷ *Id.* art. 5, 1(h).

¹²⁸ *Id.* art. 99(3); Henson, *supra* note 4, at 862.

- law enforcement;
- migration, asylum, and border control; and
- administration of justice by courts and in alternative dispute resolution, and democratic processes like voting.¹²⁹

However, the AI systems listed above are not categorized as high-risk if (1) they do not pose a significant risk of harm to health, safety, or fundamental rights of natural persons, including by not materially influencing decision-making, and (2) they are intended (a) for use in a narrow procedural task, (b) to improve a previously completed human activity, (c) to detect decision-making patterns or deviations and not meant to replace or influence the human assessment without human review, or (4) to prepare for an assessment relevant for the purposes of use cases listed in Annex III of the Act,¹³⁰ which contains a list of high-risk AI systems.¹³¹ Anytime an AI system listed in Annex III of the Act is engaged in profiling natural persons, however, it is always considered high-risk.¹³² High-risk AI systems also include those intended to be used as a safety component of a product and those covered by the EU harmonization legislation listed in Annex I of the EU AI Act.¹³³

High-risk AI systems must comply with the requirements listed in Section 2 of Chapter III of the EU AI Act.¹³⁴ This includes establishing and maintaining a risk management system¹³⁵ and establishing data governance and management practices,¹³⁶ technical documentation requirements,¹³⁷ and automatic recordkeeping over the lifetime of the system.¹³⁸ Such systems also must provide transparency and information, including “concise, complete, correct and clear” instructions to users¹³⁹ and human oversight of the system.¹⁴⁰ They must be designed with appropriate and measurable levels of accuracy and robustness and include cybersecurity measures.¹⁴¹ High-risk AI systems can be tested in real-world conditions outside AI regulatory sandboxes (see below), but only under the conditions set forth in the Act.¹⁴²

The EU AI Act includes detailed obligations for providers of high-risk AI systems, requiring implementation of quality management systems, automatically generated logs, and, in the event of non-conformity with the EU AI Act, notification to pertinent parties and immediate corrective action.¹⁴³ It also provides duties for authorized representatives of providers,¹⁴⁴ importers,¹⁴⁵

¹²⁹ EU AI Act, *supra* note 4, at annex III.

¹³⁰ *Id.* art. 6(3).

¹³¹ *Id.* annex III.

¹³² *Id.* art. 6(3).

¹³³ *Id.* art. 6(1); annex I.

¹³⁴ *Id.* art. 8.

¹³⁵ *Id.* art. 9.

¹³⁶ *Id.* art. 10.

¹³⁷ *Id.* art. 11.

¹³⁸ *Id.* art. 12.

¹³⁹ *Id.* art. 13.

¹⁴⁰ *Id.* art. 14.

¹⁴¹ *Id.* art. 15.

¹⁴² *Id.* art. 60-61.

¹⁴³ *Id.* art. 16-20.

¹⁴⁴ *Id.* art. 22.

¹⁴⁵ *Id.* art. 23.

distributors,¹⁴⁶ and deployers¹⁴⁷ of high-risk AI systems. It requires EU member states to establish notifying authorities to evaluate conformity with the Act and make reports to the Commission and other member states.¹⁴⁸

The EU AI Act requires the Commission to set up and maintain an EU database of high-risk AI systems in collaboration with the member states.¹⁴⁹ Providers of high-risk AI systems or their authorized representatives must register in the EU database¹⁵⁰ and comply with conformity assessment procedures to receive a certificate allowing that AI system to be used in the European Union.¹⁵¹ The majority of the information in this database is publicly available, including the names and contacts of the natural persons responsible for registering each AI system and those who have legal authority to represent the provider or deployer of the system.¹⁵²

Providers must draft and maintain a declaration of conformity with the EU AI Act,¹⁵³ and they must use a “CE marking” to show that it conforms to the Act.¹⁵⁴ They also must develop a post-market monitoring plan designed to actively and systematically collect, document, and analyze data throughout the AI system’s lifetime, which must be included in the technical documentation under Article 11 and Annex IV.¹⁵⁵

After the use of the system begins, data on compliance must be monitored continuously.¹⁵⁶ Any serious incidents, defined as the death of a person, serious harm to a person’s health, a serious and irreversible disruption of the management or operation of critical infrastructure, the infringement of fundamental rights under EU law, or serious harm to property or the environment,¹⁵⁷ that occur must be reported by providers to market surveillance authorities in the member states where the incident took place.¹⁵⁸ The report must be made immediately after a causal link or a reasonable likelihood of such a link between the AI system and the serious incident is determined or, at the latest, within fifteen days after the provider or deployer became aware of the incident.¹⁵⁹ If there is a serious and irreversible disruption of the management or operation of critical infrastructure, the report must be provided immediately, or at the latest within two days after the provider or deployer became aware of the incident.¹⁶⁰ In the event of the death of a person, reporting is required within ten days.¹⁶¹ National competent authorities are required to immediately notify the Commission of any serious incident.¹⁶²

¹⁴⁶ *Id.* art. 24.

¹⁴⁷ *Id.* art. 26-27.

¹⁴⁸ *Id.* art. 28-39.

¹⁴⁹ *Id.* art. 71.

¹⁵⁰ *Id.* art. 49, 71.

¹⁵¹ *Id.* art. 43-44.

¹⁵² *Id.* art. 71.

¹⁵³ *Id.* art. 47.

¹⁵⁴ *Id.* art. 3(24).

¹⁵⁵ *Id.* art. 72(8), 11; annex IV (9).

¹⁵⁶ *Id.* art. 72(2).

¹⁵⁷ *Id.* art. 3(49).

¹⁵⁸ *Id.* art. 73.

¹⁵⁹ *Id.* art. 73(8).

¹⁶⁰ *Id.* art. 73(3).

¹⁶¹ *Id.* art. 73(4).

¹⁶² *Id.* art. 73(11).

C. GPAI MODELS

The Act defines “general-purpose AI model” as a system “that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications.”¹⁶³ This includes AI models “trained with a large amount of data using self-supervision at scale,” but not those “used for research development or prototyping activities before they are placed on the market.”¹⁶⁴ Thus, GPAI models include what is commonly known as “generative AI.”¹⁶⁵

GPAI models are also referred to as “foundation models.”¹⁶⁶ “Because foundation models can be modified to numerous downstream uses, ‘no organization can fully anticipate all potential risks (or foresee all potential benefits).’”¹⁶⁷ Because of this, the risk of any particular GPAI model is difficult to predict, even if it is designed for an innocent purpose.

Early drafts of the EU AI Act did not contain any significant regulation of foundation models or generative AI.¹⁶⁸ However, ChatGPT’s release in November 2022, as discussed above, appears to have changed the understanding of regulators of the potential for risk from GPAI models.¹⁶⁹ The development of widely available generative AI models presented unprecedented regulatory challenges that fundamentally shaped the EU AI Act during its legislative process. The initial 2021 draft of the Act focused primarily on specific-use AI applications within defined sectors, but the emergence of powerful GPAI models with broad capabilities caused the introduction of an entirely new regulatory tier during the Act’s finalization.¹⁷⁰

For this reason, the EU AI Act designates GPAI models as those with or without “systemic risk.”¹⁷¹ A model will be classified as having “systemic risk” if it has “high impact capabilities,” which will be presumed “when the cumulative amount of computation used for its training measured in floating point operations [FLOPs] is greater than 10^{25} .”¹⁷² If an AI model does not meet the presumption, the Commission may also determine that it has systemic risk based on the model’s impact using the factors included in Annex XIII of the EU AI Act,¹⁷³ which contains the criteria for the designation of GPAI models with systemic risk referred to in Article 51.¹⁷⁴

Providers of GPAI models with “systemic risk” have certain obligations under the Act.¹⁷⁵ Once a model reaches the threshold for high-impact capabilities, its provider must notify the

¹⁶³ *Id.* art. 3(63).

¹⁶⁴ *Id.*

¹⁶⁵ Henson, *supra* note 4, at 858-861; Wolff, *supra* note 92, at 10.

¹⁶⁶ Arango, *supra* note 86, at 546.

¹⁶⁷ *Id.* at 553, quoting Percy Liang, Rishi Bommasani, Kathleen Creel & Rob Reich, *The Time Is Now to Develop Community Norms for the Release of Foundation Models*, STAN. U. HUM.-CENTERED A.I., May 17, 2022, <https://hai.stanford.edu/news/time-now-develop-community-norms-release-foundation-models>.

¹⁶⁸ Wolff, *supra* note 92, at 3.

¹⁶⁹ *Id.* at 4-5.

¹⁷⁰ Tambiama Madiega, *Artificial Intelligence Act*, EUROPEAN PARLIAMENTARY RSCH. SERV. (Apr. 2024).

¹⁷¹ EU AI Act, *supra* note 4, art. 51.

¹⁷² *Id.* This threshold can be written more succinctly as computational power of 10^{25} -FLOPs.

¹⁷³ *Id.* annex XIII.

¹⁷⁴ *Id.* annex I.

¹⁷⁵ *Id.* art. 55.

Commission within two weeks.¹⁷⁶ The Commission can also determine on its own or based on a qualified alert from a scientific panel that a model has high impact capabilities and, thus, has systemic risk.¹⁷⁷ In either case, if the provider disagrees that its model presents systemic risk, it can present arguments to refute the determination of systemic risk to the Commission.¹⁷⁸

The EU AI Act imposes duties on providers of all GPAI models, whether or not they include systemic risk, including maintaining technical documentation and other information on the model, compliance with codes of practice and an EU harmonized standard, and cooperation with the Commission and national authorities on the EU AI Act requirements.¹⁷⁹ Providers are also required to designate an authorized representative in the European Union.¹⁸⁰

The obligations for providers of all GPAI models, including detailed transparency about training data composition, computational resources, and energy consumption,¹⁸¹ along with the stricter requirements for large GPAI models deemed to pose “systemic risk” due to their potential widespread impact,¹⁸² specifically address the novel challenges posed by generative AI:

- Disinformation and manipulation risks: The capability to generate convincing but false content prompted rules requiring AI-generated content to be clearly identifiable, along with obligations for model providers to implement safeguards against misuse for creating deepfakes or synthetic media intended to deceive.
- Intellectual property and data governance: The practice of training models on vast datasets scraped from the internet, often without explicit consent, led to requirements that foundation model providers publish detailed summaries of copyrighted data used for training and implement appropriate licensing frameworks.
- Systemic risk and dual-use concerns: The general-purpose nature of these models, capable of both beneficial and harmful applications, brought about new risk assessment frameworks and ongoing monitoring obligations that extend beyond traditional sectoral AI regulations.

The AI Office is responsible for encouraging and facilitating the development of codes of practice for providers of GPAI models, both with and without systemic risk, at the EU level.¹⁸³

D. AI SANDBOXES

The EU AI Act encourages AI providers to experiment with new technology in safe spaces established throughout the EU called “AI regulatory sandboxes,” defined in the Act as

a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world

¹⁷⁶ *Id.* art. 52(1).

¹⁷⁷ *Id.* art. 51(1)(b).

¹⁷⁸ *Id.* art. 5(1).

¹⁷⁹ *Id.* art. 53.

¹⁸⁰ *Id.* art. 54.

¹⁸¹ *Id.*

¹⁸² *Id.* art. 52d.

¹⁸³ *Id.* art. 56.

conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision.¹⁸⁴

AI sandboxes are design spaces within a controlled environment to allow for innovation without significant risk.¹⁸⁵ They are also intended to give regulators a clear understanding of whether existing regulations are sufficient for the new systems being developed in them.¹⁸⁶ The EU AI Act gives the Commission the authority to adopt additional acts that regulate AI sandboxes.¹⁸⁷ It contains protections and limitations on the use of personal data lawfully collected for other purposes in the AI sandboxes.¹⁸⁸

The EU AI Act requires all member states, either alone or jointly, to establish at least one AI sandbox at the national level by August 2, 2026.¹⁸⁹ Member states can also establish AI sandboxes at regional or local levels.¹⁹⁰ The European Data Protection Supervisor is also authorized to establish a sandbox at the EU level.¹⁹¹

E. SUPPORT FOR PROVIDERS AND DEPLOYERS, INCLUDING SMALL AND MID-SIZE ENTERPRISES AND START-UPS

The Act includes additional support for small and mid-sized enterprises (“SMEs”) and microenterprises. Member states are required to provide SMEs, including start-ups, with priority access to AI sandboxes.¹⁹² In addition, their needs must be considered when member states establish fees for conformity assessments under Article 43.¹⁹³ The Commission must also develop simplified guidelines for microenterprises to comply with the requirements of the qualified management system required by Article 17.¹⁹⁴

F. TRANSPARENCY REQUIREMENTS

The EU AI Act establishes transparency as a general principle.¹⁹⁵ Transparency requires “that AI systems are developed and used in a way that allows appropriate traceability and explainability ...”¹⁹⁶ For all AI systems that interact directly with natural persons, it must be clear to the natural

¹⁸⁴ EU AI Act, *supra* note 4, at art. 3(55)); *see also* Henson, *supra* note 4, at 861; Lévesque, *supra* note 85, at 47.

¹⁸⁵ U.S. Chamber of Commerce Technology Engagement Center, Commission on Artificial Intelligence, Competitiveness, Inclusion, and Innovation, Report and Recommendations 87 (2023), https://www.uschamber.com/assets/documents/CTEC_AICommission2023_Report_v6.pdf (“Regulatory sandboxes are an important way for regulators and the industry to collaborate in controlled environments to test and learn how to best harness these innovations with a view toward shaping regulatory frameworks.”); Arango, *supra* note 86, at 554.

¹⁸⁶ Arango, *supra* note 86, at 554.

¹⁸⁷ EU AI Act, *supra* note 4, at art. 8.

¹⁸⁸ *Id.* art. 59.

¹⁸⁹ *Id.* art. 57(1).

¹⁹⁰ *Id.* art. 57(2).

¹⁹¹ *Id.* art. 57(3).

¹⁹² *Id.* art. 62(1).

¹⁹³ *Id.* art. 62(2).

¹⁹⁴ *Id.* art. 63.

¹⁹⁵ Iannello, *supra* note 102, at 337.

¹⁹⁶ *Key Issues: Transparency Obligations*, EU AI ACT, <https://www.euaiact.com/key-issue/5>.

person that the system is an AI system rather than another human being.¹⁹⁷ Audio, images, videos, or text content generated by an AI system, including deep fakes, must be marked as such.¹⁹⁸

G. THE REGULATORY STRUCTURE IMPLEMENTING AND ENFORCING THE EU AI ACT

The EU AI Act creates several government entities tasked with implementing the Act. The AI Office is used by the Commission to develop EU expertise and capabilities in AI, and member states are required to facilitate the AI Office's tasks.¹⁹⁹ The Commission must also establish a scientific panel of independent experts to support enforcement activities.²⁰⁰ Member states can seek support for enforcement activities from the scientific panel.²⁰¹

The European Artificial Intelligence Board ("Board") is composed of representatives from each member state, with the European Data Protection Supervisor and the AI Office serving as non-voting observers.²⁰² The Board is designed to work with the Commission and the member states to facilitate the application of the EU AI Act.²⁰³

The Act also establishes an advisory forum that includes members of industry, SMEs, start-ups, civil society, and academia, along with representatives from the Fundamental Rights Agency, ENISA, the European Committee for Standardization, the European Committee for Electrotechnical Standardization, and the European Telecommunications Standards Institute.²⁰⁴

Member states must designate internal "national competent authorities," including at least one notifying authority and one market surveillance authority.²⁰⁵ These authorities can provide guidance and advice on the EU AI Act implementation within the member state's boundaries, particularly to SMEs and start-ups.²⁰⁶ In doing so, however, they must take into account the Board's and the Commission's guidance and advice, and consult national competent authorities under other EU laws that are impacted.²⁰⁷

H. ENFORCEMENT

Violations of the AI Act are subject to steep financial penalties.²⁰⁸ For example, as discussed above, failure to comply with the unacceptable risk provisions in Article 5 can subject providers to fines up to €35 million or 7 percent of their "total worldwide annual turnover for the preceding financial year, whichever is higher."²⁰⁹ Noncompliance with certain other provisions can subject the offender to administrative fines of up to €15 million or up to 3 percent of its total worldwide annual turnover for the prior financial year, whichever is higher.²¹⁰ Providing incorrect,

¹⁹⁷ EU AI Act, *supra* note 4, art. 50.

¹⁹⁸ *Id.* art. 50; Henson, *supra* note 4, at 861; Iannello, *supra* note 102, 338-344.

¹⁹⁹ EU AI Act, *supra* note 4, art. 64.

²⁰⁰ *Id.* art. 68.

²⁰¹ *Id.* art. 69.

²⁰² *Id.* art. 65.

²⁰³ *Id.* art. 66.

²⁰⁴ *Id.* art. 67.

²⁰⁵ *Id.* art. 70.

²⁰⁶ *Id.* art. 70(8).

²⁰⁷ *Id.*

²⁰⁸ *Id.* art. 99(3); Henson, *supra* note 4, at 862.

²⁰⁹ See EU AI Act, *supra* note 4, at art. 99(3); Henson, *supra* note 4, at 862.

²¹⁰ EU AI Act, *supra* note 4, at art. 99(4).

incomplete, or misleading information to notified bodies or national authorities in reply to a request is subject to fines of up to €7.5 million or up to 1 percent of its total worldwide annual turnover for the preceding financial year, whichever is higher.²¹¹ Some commentators have opined that these penalties may impact small businesses and keep them out of the market or suppress investment and innovation in AI.²¹² However, penalties are proportional, and the amount imposed must take into account the “economic viability” of the provider.²¹³

1. MARKET SURVEILLANCE OF HIGH-RISK AI SYSTEMS

Member states’ market surveillance authorities are responsible for market surveillance of many types of high-risk AI systems, including those contained in machinery, toys, recreational watercraft, elevators, radio equipment, personal protective equipment, and medical devices.²¹⁴ They must make annual reports to the Commission and national competition authorities to assist in the application of EU law on competition.²¹⁵ Market surveillance authorities also must report any prohibited practices to the Commission.²¹⁶

For high-risk AI systems for the provision of financial services used in or by financial institutions regulated by EU law, the relevant member state’s authority supervising those institutions serves as the market surveillance authority responsible for those AI systems.²¹⁷ Member states can designate the duties of these market surveillance authorities over these high-risk AI systems to other entities at their discretion, as long as coordination with the Commission and financial laws is assured.²¹⁸

For high-risk AI systems used in law enforcement and border management, and for justice and democracy purposes, market surveillance activities must be conducted by specific supervisory authorities under other EU laws and directives.²¹⁹ Market surveillance activities for systems used by EU institutions, bodies, offices, or agencies are handled by the European Data Protection Supervisor or the EU Court of Justice.²²⁰

Surveillance activities can be coordinated between the authorities, and joint activities can be conducted.²²¹ Providers must give full access to market surveillance authorities to documentation, training, validation, and testing data sets used for the systems’ development, including application programming interfaces (“API”) and other relevant technical means and tools enabling remote access.²²² In certain circumstances, providers will be required to provide access to the source code so that the authority can assess the conformity of the system with requirements in the EU AI Act.²²³

²¹¹ *Id.* art. 99(5).

²¹² Henson, *supra* note 4, at 863.

²¹³ EU AI Act, *supra* note 4, at art. 99(1)-(2).

²¹⁴ *Id.* art. 74; annex I § A.

²¹⁵ *Id.* art. 74.

²¹⁶ *Id.*

²¹⁷ *Id.*

²¹⁸ *Id.*

²¹⁹ *Id.*

²²⁰ *Id.*

²²¹ *Id.*

²²² *Id.*

²²³ *Id.*

Market surveillance authorities are required to treat the information received from providers as confidential under the Act.²²⁴

2. MARKET SURVEILLANCE OF GPAI SYSTEMS

AI systems based on a GPAI model developed by the same provider are monitored and supervised by the AI Office, rather than the member states' market surveillance authorities.²²⁵ However, if national market surveillance authorities have reason to believe that a GPAI system can be used directly by deployers for at least one purpose classified as high-risk and is non-compliant, they must coordinate with the AI Office to investigate and notify the Board and other market surveillance authorities.²²⁶ The AI Office can share confidential information about the GPAI system with the market surveillance authorities if the authorities are unable to obtain it on their own.²²⁷

III. REGULATION OF AI IN THE UNITED STATES

As the first law of its kind in the world, the EU AI Act is likely to have a significant impact on both AI systems across the world and on the development of new AI laws in other countries.²²⁸ Companies developing AI systems that plan to market these systems within the European Union, which is one of the world's biggest markets, will need to comply with these rules.²²⁹ In addition, the "Brussels Effect" is likely to result in other jurisdictions basing their AI regulations on the EU AI Act, in whole or in part.²³⁰ As the first major governmental body to regulate this area, the European Union has likely set the standard for the rest of the world.²³¹ However, commentators have opined that other jurisdictions "could gain second-mover advantage by further improving on the EU enforcement model."²³²

Now that the European Union has established a comprehensive law governing AI, the regulatory structure of AI in the United States has become a big question, especially for AI developers and commercial users. While the EU AI Act obviously has no direct impact on regulating AI in the United States, it has been put forward as a model by many supporters of AI regulation in the United States.²³³ Currently, there is a wide variety of AI regulations in the United States from local governments, cities, and states in areas such as biometric and facial recognition, traffic technology, use of AI in employment decisions, and consumer protection; however, the

²²⁴ *Id.* art. 78.

²²⁵ *Id.* art. 75.

²²⁶ *Id.*

²²⁷ *Id.*

²²⁸ Sandra Wachter, *Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*, 26 YALE J.L. & TECH., 671, 676; Klein, *supra* note 4, at 23.

²²⁹ Wachter, *supra* note 228, at 676 ("From a business perspective, and in the interest of streamlining, it will make sense for businesses to adapt their operations to comply with the strictest laws rather than to have fragmented standards across operations.").

²³⁰ ANU BRADFORD, *THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD* (Oxford Univ. Press 2020); Wachter, *supra* note 228, at 676.

²³¹ Lévesque, *supra* note 85, at 105.

²³² *Id.*

²³³ Henry H. Perritt, Jr., *Undressing AI: Transparency Through Patents*, 33 TEX. INTELL. PROP. L.J. 137, 159 (2025), *citing* John Hillman, *Smart Regulation: Lessons from the Artificial Intelligence Act*, 37 EMORY INT'L L. REV. 775, 822 (2023) (calling for U.S. to catch up to Europe and to use EU Act as a model for regulating AI).

federal government has not enacted overarching AI legislation.²³⁴ While this article’s focus is the EU AI Act, a brief discussion of how the federal and state governments in the United States are regulating AI is appropriate as a comparison.

A. UNITED STATES’S REGULATION OF AI

President Joseph Biden issued Executive Order 14110 in October 2023, titled “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.”²³⁵ This order provided direction on regulating the impact of AI on a wide variety of topics, including immigration, diplomacy, housing, and education.²³⁶ It required federal agencies to implement over one hundred actions, “from rulemaking to developing standards to submitting reports on an AI model’s safety.”²³⁷ Private sector actors were expected to provide input into the federal agencies’ actions and regulations.²³⁸ The order provided requirements in “eight overarching policy areas”: (1) safety and security; (2) innovation, competition, and collaboration; (3) worker support; (4) AI bias and civil rights; (5) consumer protection; (6) privacy; (7) federal use of AI; and (8) international leadership.²³⁹

President Donald Trump rescinded Executive Order 14110 on January 20, 2025, the first day of his second term.²⁴⁰ However, commentators have found that “many of its requirements trickled down to the private sector through regulation by federal agencies such as the Federal Trade Commission (FTC), Food and Drug Administration (FDA), Department of Health and Human Services (HHS), and Department of Defense (DOD)” before the executive order was rescinded.²⁴¹

The U.S. Congress has not yet enacted any comprehensive AI laws.²⁴² While there have been hundreds of bills introduced in Congress that contained the term “artificial intelligence” since 2017, fewer than 30 of these bills have been enacted.²⁴³ In nearly half of those bills, the AI-focused portions related to either appropriations or national defense authorization.²⁴⁴ The most extensive of the other bills related mostly to AI activities within federal agencies and federal programs, rather than regulating or prohibiting activities in the development, use, or commercialization of AI.²⁴⁵

A debate has emerged as to whether comprehensive federal regulations “would lead to less legal uncertainty for AI developers and improve the public’s trust in AI systems, thus supporting AI innovation” or whether such legislation “would stifle innovation and competitiveness at a time

²³⁴ Lévesque, *supra* note 85, at 40.

²³⁵ Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023); Arango, *supra* note 86, at 534-540; Klein *supra* note 4, at 23.

²³⁶ Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023).

²³⁷ Arango, *supra* note 86, at 538, *citing* Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023); Henson, *supra* note 4, at 866-868.

²³⁸ Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023).

²³⁹ LAURIE HARRIS AND CHRIS JAIKARAN, CONGRESSIONAL RESEARCH SERVICE, R47843, HIGHLIGHTS OF THE 2023 EXECUTIVE ORDER ON ARTIFICIAL INTELLIGENCE FOR CONGRESS, at 1 (Apr. 3, 2024); Klein, *supra* note 4, at 24-25.

²⁴⁰ The White House, Initial Rescissions of Harmful Executive Orders and Actions (Jan 20, 2025) (<https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/>).

²⁴¹ Klein, *supra* note 4, at 23.

²⁴² HARRIS, *supra* note 5, at 40.

²⁴³ *Id.* at 4; *see also* Arango, *supra* note 86, at 543-544 (discussing two recently proposed bills in Congress attempting to regulate AI).

²⁴⁴ HARRIS, *supra* note 5, at 4.

²⁴⁵ *Id.* at 4-6, 10.

when international competition is accelerating, which could lead to negative economic and national security outcomes.”²⁴⁶ This debate will undoubtedly continue as AI develops and the impact of the EU AI Act is felt by AI developers and EU inhabitants. Some scholars have opined that the lack of a comprehensive AI law in the United States is not as problematic as others have made it seem, suggesting that existing laws and legal frameworks provide protection from many potential individual and societal harms, whether that harm is from a digital or analog cause.²⁴⁷

No matter how this debate is resolved, the EU’s AI Act will have a major impact on the development of the AI industry in the United States, as the companies developing and marketing these products in the United States will likely also market them in the European Union.²⁴⁸ When and if the federal government decides to regulate AI, it may find that coordinating U.S. regulation with the EU AI Act provides more standardization and easier implementation, at least for commercial developers and users of AI.

B. STATES’S REGULATION OF AI

Like the federal government, many states have considered legislation on AI in recent years. During the 2024 legislative session, forty-five states, Puerto Rico, the U.S. Virgin Islands, and Washington, DC introduced AI bills.²⁴⁹ The National Conference of State Legislatures tracked over 450 bills on AI in twenty-three different categories during 2024 and determined that most of this legislation focused on three areas—consumer protection, deepfakes, and government use of AI.²⁵⁰ Thirty-one states, Puerto Rico, and the U.S. Virgin Islands enacted legislation or resolutions on AI that year,²⁵¹ though only one state, Colorado, has enacted comprehensive AI legislation so far.

On May 17, 2024, Colorado passed the Colorado AI Act, which will take effect on February 1, 2026.²⁵² The Colorado AI Act includes many of the regulatory concepts included in the EU AI Act.²⁵³ It applies to legal entities doing business in Colorado that are involved in AI development or deployment.²⁵⁴ It requires the developers and deployers of high-risk AI systems to use reasonable care to avoid algorithmic discrimination and requires disclosures to consumers.²⁵⁵ Colorado also enacted a new law on June 6, 2024, that created an AI task force to recommend changes to the Colorado AI Act prior to its implementation in 2026.²⁵⁶

While not comprehensive legislation, Utah and California have also enacted important legislation on AI in 2024. On March 13, 2024, Utah enacted the Artificial Intelligence Policy Act

²⁴⁶ *Id.* at 1.

²⁴⁷ Lévesque, *supra* note 85, at 41.

²⁴⁸ Wachter, *supra* note 228, at 676.

²⁴⁹ NATIONAL CONFERENCE OF STATE LEGISLATURES, ARTIFICIAL INTELLIGENCE 2024 LEGISLATION (Sept. 9, 2024) <https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation>.

²⁵⁰ Chelsea Canada, 3 Trends Emerge as AI Legislation Gains Momentum, NAT’L. CONF. ST. LEGIS. (Jan. 23, 2025) <https://www.ncsl.org/state-legislatures-news/details/3-trends-emerge-as-ai-legislation-gains-momentum>.

²⁵¹ NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 239.

²⁵² S.B. 24-205, 74th Gen. Assemb., 2d Reg. Sess. (Colo. 2024), (https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf); Colo. Rev. Stat. §§ 611701 to 1707.

²⁵³ See Klein *supra* note 4, at 25.

²⁵⁴ S.B. 24-205, *supra* note 247.

²⁵⁵ NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 244.

²⁵⁶ S.B. 24-205, *supra* note 247.

on March 13, 2024.²⁵⁷ This law focuses on consumer protection from AI and requires certain entities to disclose the use of generative AI.²⁵⁸

California enacted the Artificial Intelligence Training Data Transparency Act on September 28, 2024.²⁵⁹ This law requires developers of generative AI systems to share the data that was used to train the system starting in 2026.²⁶⁰ The California Governor vetoed a separate bill that would have set training, safety, and enforcement standards for AI.²⁶¹

Given the growing influence of AI, state legislatures will continue to consider and enact AI legislation. This may result in a patchwork of AI laws across the United States that may stifle innovation and yet fail to provide sufficient protection. Developing uniform standards for AI across states should be considered.

IV. EXPECTATIONS FOR FURTHER DEVELOPMENT OF AI

Since the finalization of the EU AI Act, the increasing pace of AI development has validated its forward-looking regulatory approach. The increasing interest in AI, along with technological advances, many of which are now AI-enhanced, has led to rapid increases in its capabilities. This makes predicting future AI advances almost impossible. Nevertheless, there is early-stage work in research and industry that provides some indication of the direction of future AI advances and their applications.

Continued work towards developing strong AI, along with advances in weak AI modelling improvements, will undoubtedly advance AI capabilities. AI reasoning models that improve LLM performance by introducing logical reasoning have already demonstrated vast improvements in tests designed to gauge human intelligence.²⁶² Meanwhile, new algorithmic approaches have allowed AI systems to work autonomously with limited human interaction via what is termed agentic AI.²⁶³

AI processing will likely continue to become more efficient. The eventual realization of quantum and bio-computing will not only improve the efficiency of AI through optimization but also allow for new algorithmic approaches that are infeasible using classical computers.²⁶⁴ Even

²⁵⁷ S.B. 149, 2024 Gen. Sess. (Utah 2024) <https://le.utah.gov/~2024/bills/sbillenr/SB0149.pdf>; Klein, *supra* note 4, at 26-27.

²⁵⁸ Canada, *supra* note 250.

²⁵⁹ A.B. 2013, 2023-2024 Reg. Sess. (Cal., Sept. 28, 2024) <https://legiscan.com/CA/text/AB2013/id/2910882>; Klein, *supra* note 4, at 26-27 (Winter 2025).

²⁶⁰ A.B. 2013, *supra* note 254; Canada, *supra* note 250.

²⁶¹ S.B. 1047, 2023-2024 Reg. Sess. (Cal., vetoed Sept. 29, 2024) <https://legiscan.com/CA/text/SB1047/id/2919384>; Canada, *supra* note 250.

²⁶² Fengli Xu, et al., *Towards Large Reasoning Models: A Survey of Reinforced Reasoning with Large Language Models*, 14 ARXIV:2501.09686 (Jan. 14, 2025).

²⁶³ Deepak Bhaskar Acharya, et al., *Agentic AI: Autonomous Intelligence for Complex Goals—A Comprehensive Survey*, IEEE ACCESS, 18912, 18917 (2025); Xu, *supra* note 252.

²⁶⁴ Hafiz Md Hasan Babu, *Biocomputing Quantum Biocomputing in Quantum Biology Volume I: Arithmetic and Combinational Circuits*, BIOCOMPUTING QUANTUM BIOCOMPUTING 1, 6–7 (Springer 2025); Matthias Klusch, et al., *Quantum Artificial Intelligence: A Brief Survey*, 38 KI-KÜNSTLICHE INTELLIGENZ 257, 262–63 (2024).

without these advances, researchers are creating smaller, more efficient models along with streamlining AI performance with the goals of green sustainability and real-time processing.²⁶⁵

The breadth of AI functions and applications will continue to expand. As new AI methods are introduced, so are new ways in which AI can be used. AI algorithms used for image generation, for example, have led to advances in video and 3D model generation.²⁶⁶ Further advances allow for multimodal AI capable of processing multiple different types of data sources, which will allow for systems that can simultaneously examine audio, video, and text data to derive novel insights.²⁶⁷

AI enhancements will encourage adoption across non-technical industries. As of 2024, the most common use of AI has been in the technology industry for information technology support, marketing and sales, and product and service development.²⁶⁸ AI usage for manufacturing, risk, legal, and compliance, strategy, corporate finance, and supply chain and inventory management has generally been much lower across industries. This may change with newer enhancements in AI privacy, security, and explainability. For example, the development of smaller models that can be run locally on devices can aid in addressing some privacy and security concerns with using cloud-based AI for manufacturing and supply chain management.²⁶⁹ Similarly, work towards explainable AI models that allow for an understanding of exactly how answers are derived can allow for their usage for compliance in highly regulated environments.²⁷⁰ Further work is also being done to mimic the success that large foundation models have had on language by applying similar techniques to other areas, such as geography, time series, and robotics problems.²⁷¹ These can enable applications in a variety of sectors, including public, manufacturing, and decision-making domains, where location, time, and automation are desirable.

Regulation of AI will impact its growth and development. In September 2024, the EU Commission signed the Council of Europe Framework Convention on Artificial Intelligence, the first legally binding international agreement on the topic, demonstrating the Act's role in establishing international standards.²⁷² The EU AI Office has begun developing the technical standards and codes of practice that will operationalize the Act's requirements, signaling the

²⁶⁵ Lihu Chen & Gaël Varoquaux, *What Is the Role of Small Models in the LLM Era: A Survey*, 1, 2, ARXIV:2409.06857 (Sept. 12, 2024); Abdulaziz Tabbakh, et al., *Towards Sustainable AI: A Comprehensive Framework for Green AI*, 5 DISCOVER SUSTAINABILITY 408, 409 (2024).

²⁶⁶ Shamin Yazdani, et al., *Video Generative Adversarial Networks: A Review*, 55 ACM COMPUTING SURVEYS 1, 2 (2022); C. Li, et al., *Generative AI Meets 3D: A Survey on Text-to-3D in AIGC Era*, ARXIV:2305.06131 (2023).

²⁶⁷ Andrew Ng, *The Evolution of Multimodal AI: Creating New Possibilities*, 1 INT'L J. ARTIFICIAL INTELLIGENCE FOR SCI. 1, 1-2 (2025).

²⁶⁸ Maslej, *supra* note 35, at 262.

²⁶⁹ Sai Dhiresh Kilari, *The Implementation of Artificial Intelligence in the Manufacturing Industry: Manufacturing Execution Systems and Supply Chain Integration*, 25 WORLD J. ADVANCED RSCH. & REVS. 2568, 2569 (2025); Xubin Wang, et al., *Empowering Edge Intelligence: A Comprehensive Survey on On-Device AI Models*, 57 ACM COMPUTING SURVEYS 1, 8 (2025).

²⁷⁰ Andrew Nii Anang, et al., *Explainable AI in Financial Technologies: Balancing Innovation with Regulatory Compliance*, 13 INT'L J. SCI. & RSCH. ARCHIVE 1793,1794 (2024).

²⁷¹ Yuxuan Liang et al., *Foundation Models for Time Series Analysis: A Tutorial and Survey* (30th ACM SIGKDD CONF. KNOWLEDGE DISCOVERY & DATA MINING 2024); Gengchen Mai, et al., *On the Opportunities and Challenges of Foundation Models for GeoAI (Vision Paper)*, 10 ACM TRANSACTIONS SPATIAL ALGS. & SYS. 1 (2024); Zhiyuan Xu, et al., *A Survey on Robotics with Foundation Models: Toward Embodied AI*, ARXIV:2402.02385 (2024).

²⁷² Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, Council of Europe Treaty Series No. 225 (2024) <https://rm.coe.int/1680afae3c>.

transition from legislative drafting to practical implementation and enforcement. This ongoing evolution ensures that the EU AI Act will serve not as a static regulatory endpoint but as the dynamic foundation for governing AI development and deployment in an era of rapid technological change. The EU AI Act's influence is already extending beyond the European Union's borders, catalyzing global discourse on AI governance and inspiring other jurisdictions to develop their own regulatory approaches, which will impact future AI development.

V. CONCLUSION

The European Union's release of the first comprehensive regulatory framework for AI on March 12, 2024, was a groundbreaking development. The Act's risk-based focus will help ensure that fundamental human rights are protected and AI is transparent and safe, while at the same time providing support for a competitive and innovative market for AI. The Act is also serving as a template for the development of other jurisdictions' regulation of this rapidly developing technology. AI's benefits and its potential for harm are only beginning to be understood as its effects are being seen in business, education, healthcare, art, transportation, law enforcement, and international conflicts. While there is no way to accurately predict where this transformative technology will lead, the EU AI Act provides a flexible tool to help ensure that AI's development serves as a benefit to society and humanity.

Table 1: Risks explicitly regulated by the EU AI Act.

Concern	Mechanism / why it matters	Primary domains affected	Representative mitigations (EU AI Act)	Where in the EU AI Act
Deceptive manipulation and “subliminal” techniques	AI systems can materially distort behavior, leading to physical, psychological, or financial harm.	Advertising, persuasive tech, political messaging	Outright prohibition of such systems.	Art. 5(1)(a). (EUR-Lex)
Exploiting vulnerabilities (children, disability, socio-economic)	Targeting vulnerable groups undermines autonomy and amplifies harm.	Ed-tech, toys, services for vulnerable users	Outright prohibition of systems that exploit vulnerabilities.	Art. 5(1)(b). (EUR-Lex)
Social scoring	Long-term scoring leads to discriminatory or harmful treatment.	Public sector services, policing	Outright prohibition of social scoring by public authorities.	Art. 5(1)(c). (EUR-Lex)
Predictive criminal risk based on profiling/personality	Infers criminality or recidivism from traits, enabling discriminatory policing.	Law enforcement	Outright prohibition where based solely on profiling, personality traits, or past behavior.	Art. 5(1)(d). (EUR-Lex)
Building facial recognition databases via untargeted scraping	Mass scraping of faces creates de facto mass surveillance and privacy harms.	Surveillance tech vendors, data brokers	Outright prohibition on creating/expanding FR databases through untargeted scraping.	Art. 5(1)(e). (EUR-Lex)
Emotion recognition in the workplace and education	Pseudoscientific claims risk coercion and discrimination.	HR tech, schools	Outright prohibition of emotion inference in workplace and education.	Art. 5(1)(f). (EUR-Lex)
Biometric categorization by sensitive attributes	Infers race, religion, sexual orientation, etc., enabling discrimination.	Policing, border control, marketing	Outright prohibition of sensitive-attribute biometric categorization.	Art. 5(1)(g). (EUR-Lex)
Real-time remote biometric identification in public spaces (law enforcement)	Enables pervasive surveillance and chilling effects.	Law enforcement	General prohibition with narrow, enumerated exceptions for serious crimes and search for victims; strict authorization conditions.	Art. 5(1)(h), 5(2)–(7); Annex II (listed offences). (EUR-Lex)
Algorithmic bias and discrimination in high-risk AI	Biased data and design choices lead to discriminatory outcomes.	Employment, education, essential services, law enforcement, justice	Mandatory risk management and data governance (bias examination and mitigation), documentation, testing, human oversight.	Arts. 9–10 (bias controls), 14 (human oversight); high-risk areas in Annex III. (EUR-Lex , Artificial Intelligence Act)
Lack of disclosure when interacting with AI	People can be unknowingly subject to machine interactions.	Consumer services, chatbots	Providers must inform users they are interacting with AI unless obvious.	Art. 50(1). (EUR-Lex)
Deepfakes and synthetic media deception	AI-generated media can mislead and erode information integrity.	Media platforms, political communication	Machine-readable marking of AI-generated outputs by providers; deployers must disclose deepfakes and AI-	Art. 50(2), 50(4). (EUR-Lex)

Concern	Mechanism / why it matters	Primary domains affected	Representative mitigations (EU AI Act)	Where in the EU AI Act
			generated text used to inform the public.	
Transparency around emotion recognition/biometric categorization (where permitted)	Covert use infringes privacy and consent.	Retail analytics, public venues	Deployers must inform natural persons when such systems are used (subject to limited exceptions).	Art. 50(3). (EUR-Lex)
Automation bias and over-reliance	Humans over-trust automated outputs, degrading judgment.	All high-risk domains	Human oversight features and procedures to keep operators aware of automation bias and able to override/stop systems.	Art. 14(4)(b), 14(4)(d)–(e). (EUR-Lex)
Security vulnerabilities and model exploitation	Adversarial attacks, data/model poisoning, and evasion can cause harm.	Critical infrastructure, finance, healthcare, public services	Accuracy, robustness, and cybersecurity requirements; measures against data/model poisoning and adversarial examples.	Art. 15(1), 15(5). (EUR-Lex)
Traceability and auditability gaps	Without logs and documentation, accountability fails.	All high-risk domains	Technical documentation, logging, instructions for use; access for authorities; registration of high-risk systems.	Arts. 11–13, 12(1), 49, 71. (EUR-Lex)
Democratic harms from AI-driven political influence	Manipulative systems can distort elections and referenda.	Democratic processes, political campaigns	Classification as high-risk; attendant obligations (risk management, documentation, oversight); plus content-labeling duties where applicable.	Annex III(8)(b); Art. 50(2), 50(4). (Artificial Intelligence Act , EUR-Lex)
Education harms	High-stakes uses can entrench bias and harm learners.	Education and vocational training	Classified high-risk: admissions, outcome evaluation, level placement, exam-proctoring; general high-risk controls apply. Emotion recognition in education is prohibited.	Annex III(3)(a)–(d); Art. 5(1)(f). (Artificial Intelligence Act , EUR-Lex)
Workplace surveillance and algorithmic management	Monitoring and automated decisions affect livelihoods and rights.	Employment and worker management	Classified high-risk for recruitment, evaluation, monitoring; general high-risk controls and oversight apply. Emotion recognition at work is prohibited.	Annex III(4)(a)–(b); Art. 5(1)(f). (Artificial Intelligence Act , EUR-Lex)
Discrimination in essential services	AI can exclude people from benefits, credit, or insurance.	Public benefits, credit scoring, insurance, emergency response	Classified high-risk; deployers in banking/insurance must perform Fundamental Rights Impact Assessments (FRIAs); general high-risk controls apply.	Annex III(5)(a)–(d); Art. 27(1) (points 5(b)–(c)). (Artificial Intelligence Act , EUR-Lex)
Law-enforcement harms (risk scoring, evidence assessment, profiling)	Opaque tools can undermine due process and fairness.	Policing, criminal justice	Many uses are high-risk with strict controls; several practices are outright prohibited (see Art. 5).	Annex III(6)(a)–(e); Art. 5(1)(d)–(h). (Artificial Intelligence Act , EUR-Lex)

Concern	Mechanism / why it matters	Primary domains affected	Representative mitigations (EU AI Act)	Where in the EU AI Act
Migration, asylum, and border-control harms	High-stakes assessments can affect fundamental rights, including non-refoulement.	Border management, asylum processing	Classified high-risk; strict controls and, for certain uses, prohibitions/registration and FRIA requirements.	Annex III(7)(a)–(d); Art. 27; Art. 49. (Artificial Intelligence Act , EUR-Lex)
Copyright and training-data opacity in GPAI	Use of copyrighted works without compliance and opaque training corpora create legal and ethical risk.	General-purpose models, generative AI	GPAI providers must adopt copyright-compliance policies and publish a sufficiently detailed summary of training data; provide documentation to downstream providers. Additional obligations: model evaluation and adversarial testing, continuous systemic-risk assessment and mitigation, incident reporting, and cybersecurity.	Art. 53(1)(c)–(d), 53(1)(a)–(b). (EUR-Lex)
Systemic risks from frontier models (GPAI with systemic risk)	Capabilities and scale can create cross-sector harms and cascading failures.	Cross-sector		Arts. 51–55 (esp. 55(1)(a)–(d)). (EUR-Lex)
Lack of recourse for affected persons	Individuals need actionable remedies when decisions lean on high-risk AI.	All high-risk domains	Right to lodge complaints; right to an explanation when a decision is mainly based on high-risk AI output and significantly affects the person.	Arts. 85–86. (EUR-Lex)