

## **Emerging frameworks of AI regulation internationally**

**Rory Macmillan**  
**Christina Heliotis**  
**Juan J. Abad**

**February 2026**

# Contents

- I. The international AI regulation landscape.....3**
- II. Models of AI governance.....3**
  - Horizontal, economy-wide AI laws (EU, South Korea) .....3
  - Vertical or sectoral regulation (UK, U.S.) .....4
  - Principles-based or guidance-led governance (Japan) .....4
  - Cybersecurity and information-control model (China) .....5
- III. Common regulatory themes.....5**
  - Risk-based regulation .....5
  - Surveillance and sensitive uses .....6
  - Non-discrimination and bias .....6
  - Transparency and explainability.....6
  - Liability and accountability.....7
- IV. Jurisdictional snapshots .....8**
  - European Union .....8
  - United Kingdom..... 10
  - United States (federal) ..... 11
  - U.S. State: Colorado ..... 12
  - U.S. State: California..... 13
  - South Korea ..... 14
  - Japan..... 15
  - China..... 16
  - Canada..... 18
  - Brazil ..... 19
- Sources .....20**

# I. The international AI regulation landscape

Since 2022, the AI regulatory landscape has developed into several models. On one hand, some economies (European Union (EU), South Korea) are embracing comprehensive, binding AI laws that impose tiered obligations on “high-risk” uses and in the EU’s case explicitly ban certain applications [1][2]. Other jurisdictions such as the UK and Japan favor governance-based approaches: broad principles or strategic plans without immediate legal fines[3][4]. China exemplifies a state-centric, security and information-control model of AI governance. Rather than adopting a single omnibus AI Act like the EU, China regulates AI through a combination of horizontal data and cybersecurity laws and targeted AI-specific regulations focused on algorithms, deep synthesis, and generative AI[5].

These diverging approaches reflect core tensions: balancing innovation and competitiveness with safety, fundamental rights, and national security. For example, the EU embeds strict compliance obligations and significant administrative fines within a broader strategy aimed at promoting trustworthy AI. The enforcement framework is intended to be strongly deterrent: for violations of prohibited AI practices under Article 5, fines may reach €35 million or 7% of worldwide annual turnover, whichever is higher[6]. The United States, under the Trump administration, emphasizes technological leadership, deregulation, and federal authority over AI policy[7]. Recent executive action has sought to limit or preempt state-level AI laws viewed as burdensome to innovation[8].

The risk of further regulatory fragmentation is high: companies serving global markets must navigate an expanding patchwork of national and regional AI regimes, alongside potentially divergent U.S. state requirements.

This memo synthesizes the current state and emerging trends across major jurisdictions, with particular attention to cross-cutting issues such as risk management, bias and discrimination, transparency, and enforcement architecture.

## II. Models of AI governance

### Horizontal, economy-wide AI laws (EU, South Korea)

The horizontal model regulates artificial intelligence through a single, comprehensive statute that applies across largely all sectors of the economy. Rather than embedding AI rules within existing industry laws or delegating regulation to sector regulators, this approach establishes a unified framework governing the development, deployment and commercialization of AI systems.

These laws typically adopt a risk-tiered structure. Certain AI practices are prohibited outright, such as manipulative systems or specific forms of biometric surveillance. High-risk AI systems are subject to detailed compliance obligations, such as risk management systems, documentation requirements, conformity assessments, transparency measures, and human oversight safeguards. Lower-risk or minimal-risk AI systems face limited or no binding obligations, though obligations requiring transparency about the use of AI may still apply.

Enforcement is centralized and formalized. Dedicated supervisory authorities or designated national regulators oversee compliance, with powers to conduct audits, order corrective measures, and impose substantial administrative fines. Penalties can be significant, reflecting the system-wide scope of the legislation.

The EU's AI Act (2024) is the most ambitious example of this model, setting out detailed obligations for developer and deployers of high-risk AI systems and establishing a coordinated enforcement structure across Member States[6]. South Korea's Basic Act on AI also reflects an economy-wide legislative strategy[2], albeit leaving far more for later regulation.

## Vertical or sectoral regulation (UK, U.S.)

In this model, AI oversight is implemented via existing sector regulators (e.g., financial regulators, health agencies, transport safety boards). The UK's approach illustrates this: instead of new AI laws, the UK AI White Paper (2023) set out five cross-sectoral principles (fairness, transparency, safety, contestability, accountability) and directed each regulator to apply them within its domain[3]. Similarly, the U.S. has thus far generally relied on agencies such as the Food and Drug Administration (FDA) (for medical AI) or the Federal Aviation Administration (FAA) (for aviation AI), and antitrust enforcement, rather than an omnibus AI law[9].

## Principles-based or guidance-led governance (Japan)

Some countries have issued voluntary codes and guidelines rather than binding rules. Japan's AI Promotion Act (2025) and associated government guidelines are largely soft law: they declare a "basic policy" for AI use and set up a strategic planning mechanism, but do not impose fines or strict duties[4]. Industry compliance is encouraged via "AI sandboxes," ethics committees, and national AI strategies rather than statutory mandates[10]. The OECD and G7 principles similarly provide global benchmarks without legal force[11].

## Cybersecurity and information-control model (China)

China’s AI governance framework reflects a cybersecurity and information control-oriented model. Rather than adopting a single omnibus AI statute, China regulates specific AI deployment types through targeted administrative measures layered onto existing cybersecurity, data protection, and content governance laws[5][12].

The 2023 Interim Measures for the Management of Generative Artificial Intelligence Services mark the first administrative regulation specifically addressing generative AI[13]. Oversight is keyed to defined service categories, such as algorithmic recommendation systems, deep synthesis technologies, and generative AI services, and is closely tied to national security and content management objectives. Providers may be required to complete regulatory filings, undergo security assessments, and comply with labeling and content-control obligations[14].

### III. Common regulatory themes

Across governance models, several regulatory issues recur in jurisdictions’ approach to AI oversight.

#### Risk-based regulation

Most comprehensive frameworks treat risk as the organizing principle of AI governance. The EU AI Act adopts an explicit tiered structure: certain “unacceptable” practices, such as social scoring and specific forms of biometric surveillance, are prohibited[6]. High-risk systems, including AI used in medical devices, critical infrastructure and employment decisions, are subject to strict compliance obligations, including risk assessments, data governance requirements, technical documentation, human oversight, and robust safeguards. Limited-risk systems face limited transparency obligations, while minimal-risk uses remain largely unregulated.

Other jurisdictions vary in how explicitly they codify risk tiers. Brazil’s proposed AI legislation (PL 2338/2023) adopts a similarly risk-based structure[15]. The UK, by contrast, does not define statutory risk categories, instead directing sector regulators to focus on harmful or high-risk applications within their respective domains[3]. The U.S. at the federal level has not adopted formal statutory risk tiers comparable to the EU. Instead, oversight tends to occur through sector-specific regulation, procurement standards, and agency-level guidance addressing particular high-concern uses[7][16].

Even in jurisdictions without horizontal AI statutes, risk differentiation often emerges in sector-specific rules. For example, autonomous vehicle regulation, medical device

oversight, or restrictions on biometric identification tools frequently impose heightened requirements.

## Surveillance and sensitive uses

AI-enabled surveillance and biometric identification consistently attract the highest level of scrutiny. The EU AI Act places strict limits on real-time biometric identification in public spaces and subjects certain uses to narrow exceptions and authorization requirements[6]. Brazil’s proposed AI regulation similarly imposes enhanced oversight for public-sector surveillance systems[15][17]. South Korea’s Basic Act includes reporting and safety obligations for high-impact public uses of AI[2][18].

## Non-discrimination and bias

Approaches diverge on whether bias and discrimination are handled primarily through new AI-specific obligations or through existing equality, consumer protection and data protection regimes.

In a horizontal model approach, anti-discrimination is often operationalized through data governance, documentation, monitoring and accountability mechanisms for high-risk AI systems, rather than through creating a standalone equality law[6].

In a principles-based model like the UK, fairness and contestability are core pillars, and enforcement is expected to occur via regulators aligning existing legal frameworks (for example, data protection and sector conduct rules) with AI use cases[3].

In the U.S. state-law context, Colorado’s law is framed explicitly around “algorithmic discrimination,” imposing “reasonable care” duties on developers and deployers of “high-risk AI systems,” effective February 1, 2026[19][20]. California has separately clarified, through an approved regulatory action, how existing anti-discrimination rules apply to AI and automated decision systems in employment decisions[21].

## Transparency and explainability

Transparency shows up in at least three recurring forms:

First, disclosure to users that they are interacting with AI, or that content is AI-generated. South Korea’s AI Basic Act includes an “obligation to ensure AI transparency,” requiring notice to users for high-impact AI or generative AI products/services and requiring clear notice or indication for AI-generated virtual sounds/images/videos that may be difficult to distinguish from authentic materials[2]. China’s AI labeling measures similarly address labeling of AI-generated synthetic content by covered online information service providers[22].

Second, documentation and recordkeeping to enable auditability and regulatory oversight, commonly emphasized in the EU AI Act's high-risk requirements[1].

Third, explainability requirements, which vary from strong obligations (for some high-risk contexts) to more limited, context-sensitive expectations. South Korea's law illustrates a mixed approach: high-impact AI business operators must establish a plan to provide explanations for AI-generated outputs "[t]o the extent that it is technically feasible," together with documentation retention and human management/supervision measures[2].

Japan emphasizes transparency and accountability in business AI governance. For example, the Ministry of Economy, Trade and Industry (METI) AI Guidelines for Business provide for transparency and accountability, and continuous risk-assessment-based monitoring and improvement[23].

## Liability and accountability

Liability regimes are evolving. The EU has overhauled its product liability law: under Directive (EU) 2024/2853, software (including AI) is explicitly treated as a product for strict (no-fault) liability[24]. In practice, this means victims of AI-caused harm can sue manufacturers/developers without proving fault, just defectiveness. The rule applies regardless of whether software is on a device or accessed via cloud services. EU Member States must transpose the directive by December 2026, affecting all AI placed on the market after that date.

In contrast, some regimes rely on general liability and sector enforcement. South Korea's law focuses on preventing harm (safety standards) but does not overhaul tort law. Victims would still sue under ordinary negligence rules[2]. The UK's approach would channel AI harms through existing civil liability (product liability, negligence, etc.), as its plan has no new liability provisions. In the U.S., general tort rules apply. There is no federal AI-specific liability law (unless the states create one, which the Trump Executive Order now seeks to preempt)[8].

Across jurisdictions, accountability is also pursued through the institutional enforcement architecture: regulators, data-protection authorities and competition agencies share responsibility. In the EU, the European AI Office and the national market surveillance authorities are responsible for implementing, supervising and enforcing the AI Act[6]. The UK trusts the Information Commissioner's Office (ICO) and the Competition and Markets Authority (CMA) to integrate AI principles[3][25]. Japan has not created a dedicated AI regulator, with oversight remaining within existing ministerial structures[26]. In the U.S.,

enforcement lies with federal agencies, and the Trump EO created an interagency task force to sue states that “obstruct” federal AI policy[8].

## IV. Jurisdictional snapshots

Globally, AI governance is gathering pace. In addition to the jurisdictions discussed above, Brazil’s pending legislation and Canada’s reform efforts reflect continued legislative interest. Even jurisdictions associated with soft law approaches, such as the UK and Japan, are formalizing AI strategies and strengthening coordination among regulators. In contrast, at the federal level in the U.S., recent executive policy prioritizes technological leadership, deregulation, and preemption of conflicting state laws rather than the introduction of new federal AI-specific statutory obligations.

Across jurisdictions, governments are attempting to balance innovation, economic competitiveness, and national security with safeguards for safety and fundamental rights. High-profile AI harms, including discriminatory automated decision-making and synthetic media misuse, continue to drive regulatory attention. Among democratic economies, there is emerging convergence around risk management, transparency and accountability principles, often aligned with OECD and G7 frameworks.

However, fragmentation persists. The EU’s comprehensive risk-tiered model contrasts with China’s security-centered regulatory architecture, creating structural divergence in global AI governance. The likely trajectory is continued refinement and strategic adjustment as governments seek to embed guardrails while preserving innovation and competitiveness.

This section summarizes the regulatory landscape for leading jurisdictions across seven key areas: [27] [28]

- the jurisdiction’s governing legal framework
- the regulatory model (e.g., horizontal/vertical, hard/soft law)
- the approach to risk-based regulation
- bias and fundamental rights
- transparency and documentation requirements
- the approach to liability
- the enforcement architecture

### European Union

**Governing framework.** Binding horizontal regulation. The AI Act (2024/1689)[6], entering into full application on August 2, 2026, establishes a harmonized, cross-sector legal framework for AI systems based on risk classification[6]. It prohibits certain

“unacceptable risk” practices under Article 5 and imposes strict compliance obligations on providers and deployers of high-risk AI systems. The EU revised its Product Liability Directive (2024/2853), expressly confirming that software and AI systems qualify as products for strict liability purposes[24].

**Regulatory model.** Horizontal, risk-tiered statute. The AI Act applies across sectors and sets out harmonized obligations for high-risk systems, including risk management systems, data governance requirements, technical documentation, logging, human oversight, and cybersecurity safeguards.

**Risk approach.** Four-tier structure:

- Prohibited practices
- High-risk systems, subject to ex ante conformity assessments and ongoing compliance duties
- Limited-risk systems, primarily subject to transparency obligations
- Minimal-risk systems, largely unregulated

Certain biometric identification uses, particularly real-time remote biometric identification in publicly accessible spaces for law enforcement, are subject to strict limitations and narrow exceptions.

**Bias and fundamental rights.** The AI Act does not create a standalone AI discrimination statute. Instead, bias mitigation is embedded within high-risk obligations, including data quality, testing, and monitoring requirements. Broader enforcement relies on existing EU law, the Charter of Fundamental Rights and the GDPR.

**Transparency and documentation.** High-risk providers must maintain technical documentation and logs sufficient for regulatory oversight. Certain AI systems must provide user-facing disclosures, including notification that content or interactions involve AI. Transparency duties are calibrated to risk level.

**Liability.** Administrative fines may reach the higher of €35 million or 7% of global annual turnover for the most serious infringements. Moreover, under the revised Product Liability Directive, AI systems and software are expressly treated as products, enabling strict liability claims for defective AI systems.

**Enforcement architecture.** The AI Act establishes a coordinated EU-level and national supervisory structure. The European AI Office, within the European Commission, oversees implementation and directly supervises certain general-purpose AI models. Enforcement at the national level is carried out by designated competent authorities,

including market surveillance authorities responsible for monitoring compliance and enforcing prohibitions and high-risk obligations.

Governance is supported by the European Artificial Intelligence Board, a Scientific Panel of independent experts, and an Advisory Forum of stakeholders, promoting coordination and technical input across Member States.

## United Kingdom

**Governing framework.** The UK's approach, set out in its 2023 AI White Paper<sup>[3]</sup>, adopts a pro-innovation, principles-based framework rather than a binding horizontal AI law. The government articulated five cross-sector principles: safety, transparency, fairness, accountability, and contestability, to be implemented by existing regulators within their statutory mandates.

**Regulatory model.** Principles-based and regulator-led. The UK has not created a centralized AI regulator. Instead, oversight is exercised through established authorities under existing legal frameworks, including data protection law (UK GDPR), equality law, consumer protection law, product safety law, and competition law. Sector regulators have been directed to publish implementation plans explaining how they will apply the AI principles within their domains.

**Risk approach.** No formal economy-wide risk tiers. Regulators assess AI-related risks within their sectors using existing statutory powers. Risk management is decentralized and context-specific rather than codified in statute.

**Bias and discrimination.** No AI-specific discrimination regime. Algorithmic bias is addressed under existing frameworks, including the Equality Act 2010 and consumer protection law. The AI principles emphasize fairness, but enforcement relies on applying established anti-discrimination standards to AI-enabled decision-making.

**Transparency.** Transparency obligations arise primarily through data protection law and regulatory guidance. The ICO has issued guidance on explainability and automated decision-making<sup>[25]</sup>. Disclosure and documentation are encouraged through accountability requirements rather than mandated by a dedicated AI statute.

**Liability.** The UK has not adopted AI-specific liability legislation. Harm caused by AI systems would be addressed under existing negligence and product liability law.

**Enforcement architecture.** Oversight is distributed across multiple regulators, including the ICO, the CMA, and sector regulators such as Ofcom and the Civil Aviation

Authority. The UK has also established an AI Security Institute to support evaluation and testing of advanced AI systems[29].

## United States (federal)

**Governing framework.** No comprehensive federal AI statute is in force. Federal AI oversight operates through agency authority, executive policy, and sector-specific regulation. On December 11, 2025, President Trump issued an Executive Order (EO) establishing a “minimally burdensome” national AI policy framework and directing federal agencies to promote U.S. AI leadership[8]. The EO instructs the Department of Justice to establish an AI Litigation Task Force to evaluate and challenge state AI laws deemed inconsistent with federal policy, including on preemption and interstate commerce grounds.

**Regulatory model.** Sectoral based. The EO articulates a preference for uniform national standards and directs review of state AI laws, but it does not itself invalidate state statutes[8]. In practice, AI governance occurs through existing agency mandates: the FDA regulates AI-enabled medical devices, the FAA oversees aviation safety, the Federal Trade Commission (FTC) enforces unfair or deceptive practices, the U.S. Equal Employment Opportunity Commission (EEOC) applies civil rights laws to employment AI, and other agencies regulate AI within statutory authority.

**Risk approach.** No risk classification exists at the federal level.

**Bias and discrimination.** There is no federal AI-specific anti-discrimination statute. Agencies such as the EEOC and the U.S. Department of Justice (DOJ) enforce existing civil rights statutes, including Title VII of the Civil Rights Act of 1964 and the Americans with Disabilities Act, against discriminatory automated decision-making. The FTC has also brought enforcement actions under Section 5 of the FTC Act involving allegedly biased or deceptive algorithmic practices.

**Transparency.** Transparency expectations arise primarily through consumer protection, securities disclosure, and sector-specific regulation. NIST’s AI Risk Management Framework provides voluntary guidance on documentation and risk mitigation[30].

**Liability.** No AI-specific federal liability regime has been enacted. Harm caused by AI systems is addressed under existing tort law, product liability principles, civil rights statutes, and consumer protection law.

**Enforcement architecture.** There is no dedicated federal AI regulator. Enforcement authority remains distributed across agencies, including the FTC, DOJ, the U.S.

Securities and Exchange Commission, FDA, FAA, Federal Communications Commission, and others.

## U.S. State: Colorado

**Governing framework.** Colorado’s SB24-205, enacted in May 2024 and effective February 1, 2026, establishes the first comprehensive U.S. state framework specifically addressing “algorithmic discrimination” in high-risk AI systems[19][31]. The law applies to developers and deployers of high-risk AI systems used in consequential decisions, including employment, housing, lending, education, and healthcare.

**Regulatory model.** The law imposes affirmative obligations on private-sector actors using covered high-risk systems. It is enforced primarily by the Colorado Attorney General and operates alongside existing state civil rights and consumer protection laws.

**Risk approach.** The statute defines “high-risk artificial intelligence systems” as those used in consequential decisions affecting access to significant life opportunities. Obligations apply specifically to these systems rather than to AI generally.

**Bias and discrimination.** Algorithmic discrimination is the statute’s central focus. Developers and deployers must exercise “reasonable care” to prevent discriminatory outcomes against protected classes. The law imposes proactive duties, including impact assessments, risk management measures, and ongoing monitoring.

**Transparency.** Deployers of high-risk systems must provide notice when such systems are used in consequential decisions and must offer individuals meaningful information about the role of the system in decision-making. Documentation and risk assessment requirements support regulatory review.

**Liability.** The statute does not create a private right of action or a new strict liability regime. Instead, violations are enforceable by the Colorado Attorney General and treated as deceptive trade practices under Colorado law, subject to civil penalties assessed per violation. The Act operates alongside existing civil rights and consumer protection statutes, under which individuals may pursue remedies. The statute also provides an affirmative defense where developers or deployers demonstrate compliance with specified risk management and documentation requirements.

**Enforcement architecture.** The Colorado Attorney General is the exclusive enforcement authority under the Act. The statute does not establish a dedicated AI regulator but relies on existing state enforcement mechanisms under the Colorado Consumer Protection Act.

## U.S. State: California

**Governing framework.** California does not have a comprehensive horizontal AI statute comparable to the EU AI Act. Instead, AI governance operates through a combination of privacy law, civil rights law and targeted AI-specific statutes[32]. The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), regulates automated decision-making where personal information is involved[33][34]. In addition, California has enacted issue-specific AI legislation addressing transparency and generative AI.

**Regulatory model.** Incremental and layered. Rather than adopting a single AI Act, California has pursued targeted statutory interventions layered onto its privacy and consumer protection framework. This model emphasizes transparency, accountability and reporting obligations rather than ex ante licensing or conformity assessment.

**Risk approach.** California does not employ a formal AI risk-tier classification system. Oversight is contextual and activity-based. High-impact uses such as employment screening, consumer profiling, or consequential decision-making involving personal data are addressed through privacy, civil rights and consumer protection statutes rather than through predefined “high-risk” categories.

**Transparency.** Transparency is the defining feature of California’s AI approach. For example:

- The California AI Transparency Act[35] (effective January 1, 2026) requires certain “Covered Providers” (publicly accessible AI systems with more than one million monthly users) to disclose when content has been generated or materially modified by AI. Violations may result in civil penalties of up to \$5,000 per violation per day.
- The Generative AI Training Data Transparency Act[36] (effective January 1, 2026) requires developers of generative AI systems to publish a high-level summary of the datasets used to train their models. Required disclosures include categories and sources of training data, whether copyrighted or otherwise protected material is included, whether personal information as defined under the CCPA was used, and whether datasets were purchased or licensed.

**Frontier model legislation.** In 2025, California enacted SB 53, the Transparency in Frontier Artificial Intelligence Act[37], following the Governor’s veto of SB 1047, a more stringent frontier AI bill. SB 1047 would have imposed significant safety obligations on developers of powerful models, including mandatory shutdown capabilities, cost-

based penalties tied to model development, and mandatory reporting of certain safety incidents to the Attorney General[38].

After vetoing SB 1047, the Governor convened a policy working group on frontier AI models. SB 53 reflects a policy recalibration: instead of strict pre-deployment safety mandates, it emphasizes transparency and reporting. Developers must publicly disclose safety protocols, penalties are capped rather than tied to development cost, and a reporting mechanism was created through the Office of Emergency Services for potential critical safety incidents[38].

**Bias and discrimination.** California addresses discriminatory AI outcomes through existing civil rights statutes[21].

**Liability.** No comprehensive AI-specific strict liability regime has been adopted. AI-related liability arises under existing privacy, consumer protection, and civil rights law.

**Enforcement architecture.** Enforcement authority is shared between the California Attorney General and the California Privacy Protection Agency. Additional enforcement may occur through civil rights and consumer protection channels. California has not established a dedicated AI regulatory agency.

## South Korea

**Governing framework.** South Korea adopted the Basic Act on the Development of Artificial Intelligence and Establishment of Trust in January 2025, which took effect on January 2026[2]. The Act consolidates prior legislative proposals into a unified national framework and positions AI development as a strategic economic priority. It defines AI systems broadly and applies to both developers and deployers operating in South Korea.

**Regulatory model.** The Act combines industrial policy measures including support for research and development, talent development, and regulatory sandboxes with mandatory safety and transparency obligations for designated high-impact AI systems. The Act provides for detailed implementation through subordinate legislation, including Presidential Decrees and ministerial regulations, some of which remain under development.

**Risk approach.** Targeted “high-impact” designation rather than EU-style risk tiers. The government may designate certain AI applications as high-impact based on their societal or safety implications. Designated systems are subject to enhanced

obligations, including registration, testing, monitoring and incident reporting. Other AI systems remain subject to lighter, principle-based expectations.

**Bias and discrimination.** The Act emphasizes fairness, transparency and prevention of social harm but does not establish a standalone AI discrimination regime. Bias-related harms are addressed through existing legal frameworks, including employment and privacy law, supplemented by governance and oversight requirements for high-impact systems.

**Transparency.** Operators of designated high-impact AI systems must provide user notice and maintain documentation sufficient to demonstrate compliance. The framework also contemplates labeling requirements for AI-generated synthetic content and includes recordkeeping obligations.

**Liability.** The Basic Act does not create a new AI-specific tort or strict liability regime. Civil liability continues to be governed by existing Korean law, while the Act primarily relies on administrative enforcement tools, including corrective orders and fines.

**Enforcement architecture.** Oversight is coordinated through a national AI policy structure led by the Ministry of Science and Information and Communication Technology, with sector ministries responsible for implementation within their domains. The framework applies to AI systems provided within South Korea, including by foreign providers operating in the Korean market.

## Japan

**Governing framework.** Japan enacted the Act on the Promotion of Research, Development and Utilization of Artificial Intelligence-Related Technologies in 2025<sup>[4]</sup>. The Act establishes national AI policy objectives and creates a Cabinet-level coordination framework for AI strategy. It requires the adoption of a Basic Policy to guide medium-term implementation but does not create a comprehensive regulatory regime comparable to the EU AI Act.

**Regulatory model.** Principles-based and policy-driven. The Act articulates high-level principles and commits the government to promoting AI development, standard-setting and international cooperation. It does not impose categorical prohibitions, licensing requirements or administrative fines. Compliance expectations are operationalized primarily through government guidelines, industry standards, and public-private coordination rather than binding AI-specific mandates.

**Risk approach.** No formal risk-tier structure. The Act identifies priority fields for AI development and acknowledges the need to address safety and societal risks, but

detailed oversight mechanisms are addressed through sector-specific law and administrative guidance. Regulation of higher-risk applications occurs under existing legal frameworks rather than through AI-specific prohibitions.

**Bias and human rights.** The Act references respect for fundamental rights and ethical principles but does not establish AI-specific anti-discrimination obligations. Bias-related harms are addressed under existing legal regimes, including the Act on the Protection of Personal Information[39] and labor and civil law frameworks. Government-issued AI ethics and governance guidelines encourage fairness and responsible data practices.

**Transparency.** Transparency and explainability are promoted through policy guidance rather than statutory mandates. Ministries, including METI, have issued voluntary guidance encouraging documentation, risk assessment, and responsible disclosure practices, particularly for public-sector AI deployments[23].

**Liability.** Japan has not adopted AI-specific liability legislation. Civil liability continues to be governed by existing tort and product liability law, including the Product Liability Act. No strict liability regime specific to AI systems has been introduced.

**Enforcement architecture.** The Act does not establish a dedicated AI enforcement authority or a penalty-based compliance regime. It places a general obligation on relevant actors to make reasonable efforts to align AI development and deployment with the Act’s guiding principles and to cooperate with government inquiries. However, it does not create specific administrative fines or criminal penalties for non-compliance. Oversight remains coordinated through Cabinet-level policy structures, with any binding enforcement occurring under existing sector-specific or general laws.

## China

**Governing framework.** No single omnibus AI statute. China regulates AI through a combination of cybersecurity, data governance, and content control laws[5], including the Cybersecurity Law[40], Data Security Law[41], and Personal Information Protection Law[42]. AI-specific administrative measures include the Provisions on Algorithmic Recommendation (2022)[43], the Deep Synthesis Provisions (2023)[44][22], and the Interim Measures for the Management of Generative AI Services (2023)[13].

**Regulatory model.** Cybersecurity and content governance-oriented model. AI systems are generally regulated as “internet information services” and are subject to filing, security assessment, and content management obligations. Providers of certain services must register algorithms, implement internal compliance mechanisms, and adhere to state content standards. Regulation is embedded within China’s broader

digital governance and cybersecurity framework rather than structured as a cross-sector AI statute.

**Risk approach.** Targeted and activity-specific rather than tier-based. The framework does not establish formal economy-wide risk categories comparable to the EU. Instead, heightened oversight applies to defined service types, including algorithmic recommendation systems, deep synthesis technologies, and generative AI services. Services with “public opinion attributes” or significant social impact may be subject to security assessments and regulatory filings prior to deployment.

**Bias and discrimination.** China has not enacted a standalone AI discrimination statute. The generative AI measures require providers to avoid discriminatory outputs and to respect personal information and intellectual property rights. Broader equality protections arise under existing civil and administrative law frameworks.

**Transparency.** AI-generated synthetic content must be labeled in accordance with 2025 labeling rules issued by the Cyberspace Administration of China[22]. Providers are required to disclose certain operational information to regulators and maintain records. Transparency obligations are oriented toward regulatory supervision and content governance rather than user-facing explanation rights.

**Liability.** The framework relies primarily on administrative enforcement. Violations may result in corrective orders, fines, suspension of services, or other penalties under cybersecurity, data protection or related laws. Civil liability for AI-related harm is governed by existing tort and civil code provisions rather than by an AI-specific strict liability regime.

**Enforcement architecture**[13]. The Cyberspace Administration of China (CAC) plays a leading role in supervising generative AI and algorithmic services, in coordination with other ministries acting within their respective statutory mandates. Under the Interim Measures for Generative AI Services, regulators are authorized to conduct security assessments, supervisory inspections, and require corrective measures[13].

Article 21 of the Interim Measures for the Management of Generative AI Services provides that violations are penalized under existing laws, including the Cybersecurity Law, Data Security Law, and Personal Information Protection Law[13]. Authorities may issue warnings, order rectification, suspend services, or impose fines. Serious violations may trigger administrative sanctions or criminal liability under applicable law.

Enforcement is therefore administrative and multi-agency, grounded in China’s broader cybersecurity and data governance framework rather than a standalone AI-specific penalty regime.

## Canada

**Governing framework.** No federal AI-specific statute is currently in force. Bill C-27 (2022), which included the proposed Artificial Intelligence and Data Act (AIDA), did not complete the legislative process before Parliament was dissolved[45]. As of 2026, AI is regulated through existing legal frameworks rather than a comprehensive AI law.

**Regulatory model.** Fragmented and sector-based. Oversight operates through existing statutes, including the Personal Information Protection and Electronic Documents Act (PIPEDA), federal and provincial privacy laws, and sector regulators. No centralized AI regulator has been established.

**Risk approach.** No statutory risk-tier framework applies to private-sector AI. The proposed AIDA would have introduced obligations for high-impact systems, but these provisions were not enacted. However, Canada has issued a Directive on Automated Decision-Making that imposes risk-mitigating requirements on federal government use of automated decision systems, including mandatory impact assessments and transparency obligations[46].

**Bias and discrimination.** AI-related discrimination is addressed under existing human rights and employment laws, including the Canadian Human Rights Act and provincial codes. Privacy regulators may review automated decision-making systems where they involve the processing of personal information, under existing data protection laws such as PIPEDA and provincial privacy statutes[47].

**Transparency.** Transparency obligations arise primarily through privacy law and public-sector directives. The Treasury Board's Directive on Automated Decision-Making imposes binding requirements on federal government systems. In contrast, private-sector AI oversight relies on existing privacy law, supplemented by non-binding guidance from the Office of the Privacy Commissioner[48].

**Liability.** Canada has not adopted AI-specific liability reforms. Harm caused by AI systems is addressed under existing tort, consumer protection and product liability frameworks.

**Enforcement architecture.** Enforcement authority remains distributed across existing institutions, including the Office of the Privacy Commissioner, the Competition Bureau, and sector regulators. Provincial privacy commissioners also play a role. No dedicated AI supervisory authority exists.

## Brazil

**Governing framework.** Pending comprehensive AI legislation. Bill 2338/2023, approved by the Federal Senate in December 2024, proposes a national AI framework based on risk classification<sup>[15][17]</sup>. As of 2026, the bill awaits consideration in the Chamber of Deputies and has not yet entered into force. In the interim, AI is regulated under existing legal frameworks, including Brazil's General Data Protection Law (LGPD), consumer protection law and sector-specific regulation.

**Regulatory model.** Proposed horizontal, risk-based statute. If enacted, Bill 2338/2023 would establish a comprehensive AI regulatory framework, integrating human rights safeguards, transparency obligations, and risk management requirements. The bill contemplates institutional coordination between a designated AI authority and existing regulators, including the National Data Protection Authority (ANPD).

**Risk approach.** Explicitly tiered in draft form. The bill classifies AI systems based on potential risk, prohibits certain excessive-risk practices, and imposes enhanced obligations on high-risk systems, including impact assessments, documentation and transparency measures. Certain public-sector uses, including biometric identification in security contexts, would be subject to heightened safeguards rather than categorical prohibition.

**Bias and discrimination.** The draft framework integrates anti-discrimination safeguards into high-risk compliance obligations. Developers and deployers of high-risk systems would be required to conduct impact assessments addressing potential discriminatory effects, aligning AI oversight with Brazil's constitutional protections and existing equality law.

**Transparency.** The bill includes transparency obligations requiring disclosure when individuals are subject to automated decision-making and mandates documentation and traceability for high-risk AI systems.

**Liability.** The proposed legislation includes administrative penalties for non-compliance, including fines, while maintaining the applicability of existing civil, consumer protection and data protection liability regimes to AI-related harm.

**Enforcement architecture.** The proposed legislation grants the competent authority broad supervisory and corrective powers. These include the authority to require reclassification of an AI system's risk level, mandate algorithmic impact assessments, and order mitigation of serious incidents. Administrative sanctions may include warnings, public disclosure of violations, fines of up to R\$ 50 million per infraction (or up to 2% of the company's prior-year revenue), suspension of sandbox participation,

restrictions on data processing, and temporary or permanent suspension of system development or deployment.

## Sources

### European Union

- [6] Regulation (EU) 2024/1689 (Artificial Intelligence Act), Official Journal of the European Union, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- [1] European Commission, AI Act Overview, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- [24] Directive (EU) 2024/2853 on Liability for Defective Products, <https://eur-lex.europa.eu/eli/dir/2024/2853/oj>

### United Kingdom

- [3] UK Government, A Pro-Innovation Approach to AI Regulation (AI White Paper, 2023), <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach>
- [25] Information Commissioner's Office (ICO), Guidance on AI and Data Protection, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/>
- [29] AI Security Institute, <https://www.gov.uk/government/organisations/ai-security-institute>

### United States (Federal)

- [8] Executive Order, Eliminating State Law Obstruction of National Artificial Intelligence Policy (Dec. 11, 2025), <https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/>
- [16] OMB Memorandum M-25-22, <https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf>
- [7] America's AI Action Plan, <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>
- [30] NIST, Artificial Intelligence Risk Management Framework, <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>
- [9] U.S. Food and Drug Administration, Artificial Intelligence and Machine Learning in Medical Devices, <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-software-medical-device>

### **U.S. State of Colorado**

- [19] Colorado SB24-205 (Artificial Intelligence Act), Enrolled Act, [https://content.leg.colorado.gov/sites/default/files/2024a\\_205\\_signed.pdf](https://content.leg.colorado.gov/sites/default/files/2024a_205_signed.pdf)
- [31] Skadden, Colorado’s Landmark AI Act, <https://www.skadden.com/insights/publications/2024/06/colorados-landmark-ai-act>
- [20] KPMG, “AI Regulation: Colorado Artificial Intelligence Act (CAIA)”, <https://kpmg.com/us/en/articles/2024/ai-regulation-colorado-artificial-intelligence-act-caia-reg-alert.html>

### **U.S. State of California**

- [33] California Privacy Protection Agency (CPPA), Proposed Regulations Text, CCPA Updates (Cyber Risk, Automated Decision-making, and Other Modifications) [https://cppa.ca.gov/regulations/pdf/ccpa\\_updates\\_cyber\\_risk\\_admt\\_mod\\_txt\\_pro\\_reg.pdf](https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_mod_txt_pro_reg.pdf)
- [34] Skadden, “California Finalizes CPPA Regulations” (Oct. 2025), <https://www.skadden.com/insights/publications/2025/10/california-finalizes-cppa-regulations>
- [35] AB 853 – California AI Transparency Act, [https://calmatters.digitaldemocracy.org/bills/ca\\_202520260ab853](https://calmatters.digitaldemocracy.org/bills/ca_202520260ab853)
- [36] AB 2013 – Generative AI: Training Data Transparency Act, [https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\\_id=202320240AB2013](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2013)
- [37] SB 53 – Artificial Intelligence Models: Large Developers, [https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\\_id=202520260SB53](https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB53)
- [21] California Civil Rights Council – AI Employment Regulation, <https://calcivilrights.ca.gov/2025/06/30/civil-rights-council-secures-approval-for-regulations-to-protect-against-employment-discrimination-related-to-artificial-intelligence/>
- [32] Georgetown CSET, California’s Approach to AI Governance, <https://cset.georgetown.edu/article/californias-approach-to-ai-governance/>
- [38] ETO (Emerging Technology Observatory), “California AI Bills,” <https://eto.tech/blog/california-ai-bills/>

### **South Korea**

- [2] AI Basic Act of the Republic of Korea, <https://aibasicact.kr/>

- [18] Reuters, South Korea Launches Landmark AI Law, <https://www.reuters.com/world/asia-pacific/south-korea-launches-landmark-laws-regulate-ai-startups-warn-compliance-burdens-2026-01-22/>

## Japan

- [4] AI Promotion Act (Reference Translation), <https://www.kojimalaw.jp/wp/wp-content/uploads/2025/09/Japan-AI-Promotion-Act-KOJIMA-LAW-OFFICES-jp-en-reference-translation.pdf>
- [23] Ministry of Economy, Trade and Industry (METI), AI Guidelines for Business, [https://www.meti.go.jp/shingikai/mono\\_info\\_service/ai\\_shakai\\_jisso/pdf/20241226\\_1.pdf](https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20241226_1.pdf)
- [39] Act on the Protection of Personal Information (APPI), <https://www.ppc.go.jp/en/legal/>
- [26] White & Case, AI Watch: Japan, <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-japan>

## China

- [5] White & Case, AI Watch: China, <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china>
- [40] Cybersecurity Law (English Translation), <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>
- [41] Data Security Law (English Translation), <https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/>
- [42] Personal Information Protection Law (PIPL), [http://en.npc.gov.cn.cdurl.cn/2021-12/29/c\\_694559.htm](http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm)
- [43] Provisions on Algorithmic Recommendation, <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/>
- [12] Provisions on the Administration of Algorithmic Recommendation for Internet Information Services, <https://www.chinalawtranslate.com/en/algorithms/>
- [13] Interim Measures for the Management of Generative Artificial Intelligence Services, <https://www.chinalawtranslate.com/en/generative-ai-interim/>
- [22] Measures for Labeling of AI-Generated Synthetic Content, <https://www.chinalawtranslate.com/en/ai-labeling/>

- [44] Library of Congress, China: Deep Synthesis Provisions, <https://www.loc.gov/item/global-legal-monitor/2023-04-25/china-provisions-on-deep-synthesis-technology-enter-into-effect/>

### **Canada**

- [45] Bill C-27, <https://www.parl.ca/LegisInfo/en/bill/44-1/c-27>
- [46] Directive on Automated Decision-Making, <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>
- [47] Personal Information Protection and Electronic Documents Act (PIPEDA), <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>
- [48] Office of the Privacy Commissioner of Canada – Artificial Intelligence, <https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/>

### **Brazil**

- [15] Brazil AI Bill (PL 2338/23) Overview, <https://artificialintelligenceact.com/brazil-ai-act/>
- [17] White & Case, AI Watch: Brazil, <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-brazil>

### **International Standards and Other Sources**

- [11] OECD, OECD AI Principles (2019), <https://oecd.ai/en/ai-principles>
- [10] Asian Development Bank, Regulatory Sandbox Commentary, <https://blogs.adb.org/blog/let-ai-developers-play-regulatory-sandbox>
- [27] IAPP, Global AI Law and Policy Tracker – Highlights and Takeaways, <https://iapp.org/news/a/global-ai-law-and-policy-tracker-highlights-and-takeaways>
- [28] IAPP, Global AI Legislation Tracker, <https://iapp.org/resources/article/global-ai-legislation-tracker>