Legislation concerning AI an overview worldwide

Chair: Silvia Bortolotti, Buffa Bortolotti & Mathis, Turin; Vice-Chair and Secretary General IDI, IDI country expert for agency, distribution and franchising in Italy

EU: Francesca Hennig-Possenti, AI and Data Senior Legal Counsel at John Deere, Manheim

CHINA: Alina Quach, Asiallians, Paris – Beijing; IDI country expert for agency and distribution in China

USA: Alan Greenfield, Greenberg Traurig, LLP, Aspen

BRAZIL: Luciana Bassani, Gameleira, Pelagio, Fabiao e Bassani, Rio de Janeiro; IDI country expert for franchising in Brazil

CHILE: Cristóbal Porzio, Porzio, Rios, Garcia & Asociados, Santiago; IDI Country Experts Representative, IDI country expert for distribution in Chile

CANADA: Peter Snell, Cassels Brock & Blackwell LLP, Vancouver

Turin, June 7, 2025

European Union

EU AI Act

Francesca Hennig-Possenti

Data and AI Senior Counsel

John Deere Gmbh & Co. KG

AI Regulation

- Directly applicable horizontal regulation (published on **12 July 2024**) entered into force on **August 1, 2024**
- Applies to all AI released in the European Union
- Applies extraterritorially when outputs are used in Europe
- Provides a technology risk approach:

Prohibited Artificial Intelligence

High risk artificial intelligence

GPAI (Medium Risk – High Impact)

Regular Artificial Intelligence (no/low risk)

FHP image

Artificial intelligence is a fluid concept characterized by rapidly advancing technology and diverse application areas

AI Definition

AI system' means 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;

.

Prohibited Artificial Intelligence

Art. 5 of the AI Regulation prohibits AI from

subliminal influencing of consciousness or intentionally manipulative **or deceptive techniques**

exploit the vulnerability or vulnerability of a natural person or a specific group of persons

Detrimental evaluation or classification of natural persons (derived or predicted personal characteristics)

Criminal profiling / prosecution (with exceptions) eg. biometric real-time remote identification systems

Facial recognition through the untargeted reading of facial images from the Internet or CCTV

Sentiment analysis of a natural person at the workplace and educational institutions (with exceptions)

Biometric AI eg. to **determine political/religious/sexual attitudes**

Real-time remote biometric identification systems in publicly accessible spaces for law enforcement

High Risk AI Systems

Definition of High Risk in Art. 6 AI Act:

It is a product covered by the Regulation in Annex I

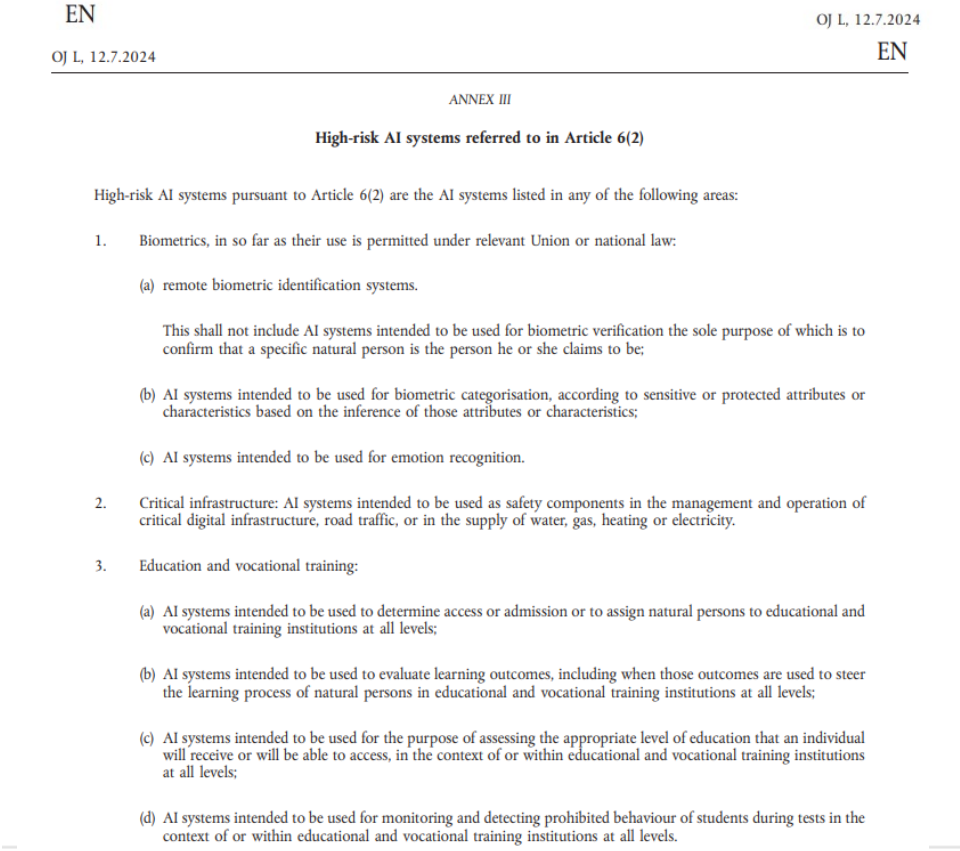
Is intended for use as a safety component for the products listed in Annex I

AND

The legislation in Annex I requires a third-party assessment.

OR

where listed in Annex III (critical infrastructure/targeted activities)



EN

OJ L, 12.7.2024

OJ L, 12.7.2024

EN

ANNEX III

High-risk AI systems referred to in Article 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometrics, in so far as their use is permitted under relevant Union or national law:

   (a) remote biometric identification systems.

   This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be;

   (b) AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics;

   (c) AI systems intended to be used for emotion recognition.

2. Critical infrastructure: AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity.

3. Education and vocational training:

   (a) AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels;

   (b) AI systems intended to be used to evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels;

   (c) AI systems intended to be used for the purpose of assessing the appropriate level of education that an individual will receive or will be able to access, in the context of or within educational and vocational training institutions at all levels;

   (d) AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.

High Risk Systems classified in Annex III

- Biometric systems (if not used as keys)
- Biometrics for categorization
- Sentiment analysis outside the work environment/education
- Critical infrastructures
- Education and training
- HR
- Access to public services
- Creditworthiness/credibility
- Life and health insurance
- Emergency Call Selection/Answering/Management
- Law enforcement (e.g. profiling, risks, evidence assessment)
- Migration (e.g., border control, security risk assessment, application assessment)
- Judicial decisions
- Influencing elections

AI generated image

High Risk AI Requirements

High-risk AI and some GPAI must meet requirement:

Risk management (Art. 9)

Data Governance/Design Governance (Art. 1)

Technical documentation (Art. 11)

Record Keeping (Art. 12) - logs

Transparency and Info (Art. 13)

Human Oversight (Art. 14)

Accuracy, Robustness/Cybersecurity (Art. 15)

Quality (art. 17)

General Purpose AI

GPAI (Art. 51) with systemic risk if

- As high impact capability
- Based on a ad hoc decision
- Has high impact capabilities and more than 10^25 FLOPS
- Commission to provide thresholds, benchmarks and indicators Annex XIII
- Notification if requirements of Art. 51 are met
- Need to prove that it has no systemic risk

Article 51(1), point (a), the Commission shall take into account the following criteria:

- (a) the number of parameters of the model;
- (b) the quality or size of the data set, for example measured through tokens;
- (c) the amount of computation used for training the model, measured in floating point operations or indicated by
- a combination of other variables such as estimated cost of training, estimated time required for the training, or
- estimated energy consumption for the training;
- (d) the input and output modalities of the model, such as text to text (large language models), text to image,
- multi-modality, and the state of the art thresholds for determining high-impact capabilities for each modality, and
- the specific type of inputs and outputs (e.g. biological sequences);
- (e) the benchmarks and evaluations of capabilities of the model, including considering the number of tasks without
- additional training, adaptability to learn new, distinct tasks, its level of autonomy and scalability, the tools it has
- access to;
- (f) whether it has a high impact on the internal market due to its reach, which shall be presumed when it has been
- made available to at least 10 000 registered business users established in the Union;
- (g) the number of registered end-users

Obligations for providers of GPAI

No systemic Risk

- Provide technical documentation including training and testing
- Draw up, keep and make available up to date information on AI System
- Comply with copyright and related rights
- Detailed summary about content used for training (exceptions for open source but not for GPAI with systemic risks)
- Code of practice demonstrating compliance with the AI Act

Systemic Risk

Model evaluation (GAN testing)

Assess and mitigate possible risks

Keep track of, document and report relevant information about accidents and correction measures

Cybersecurity protection

Compliance with harmonized standards

Obligations for importers and dealers

Importers

- Conformity assessment
- Certification
- Technical documentation
- Evaluation of the system
- Sales top in case of errors/hazards
- Information Provision
- Documentation
- Representation of the manufacturer

Dealers

- Review of the EU declaration of conformity
- Do not use/remove from sale if faulty
- Taking corrective action
- Cooperation with authorities

AI generated image

Obligations for operators (users)

- Human supervision
- Exercise control over data entry (representative -> intended goal)
- Monitoring AI operations
- Vendors provide information about AI behavior and errors
- Instructions
- Information on market surveillance
- Record keeping (6 m)
- Information of employee representatives (works councils)
- Conducting the Data Protection Impact Assessment
- Judicial authorization for certain cases
- Inform data subjects

Fines and Penalties

- Non compliance with Art. 5 up to 35 Mio or 7% of total worldwide turnover for the preceding financial year
- Non compliance with other requirements 15 Mio or 3% of worldwide financial turnover for the preceding financial year
- Incorrect, incomplete or misleading information 7.5 Mio or 1% of worldwide turnover for the preceding financial year

FHP image

THANK YOU

AI legal framework in China

Alina Quach
Avocat au Barreau de Paris
Hong Kong Foreign registered lawyer
ASIALLIANS LLP
Country expert for agency and distribution
alina.quach@asiallians.com

- No comprehensive definition of AI:

  China has not established a single, comprehensive definition of artificial intelligence (AI) in its laws and regulations. However, several regulations address different aspects of AI technologies and aim to manage the risks associated with AI-generated content and ensure national and social security.

- Legislative intent:

  - Promote technological innovation in AI: Encouraging advancements and research in AI technologies.

  - Facilitate the healthy development of the AI industry: Ensuring sustainable growth and ethical practices.

  - Regulate AI product and service development, provision, and use activities: Establishing standards for AI applications.

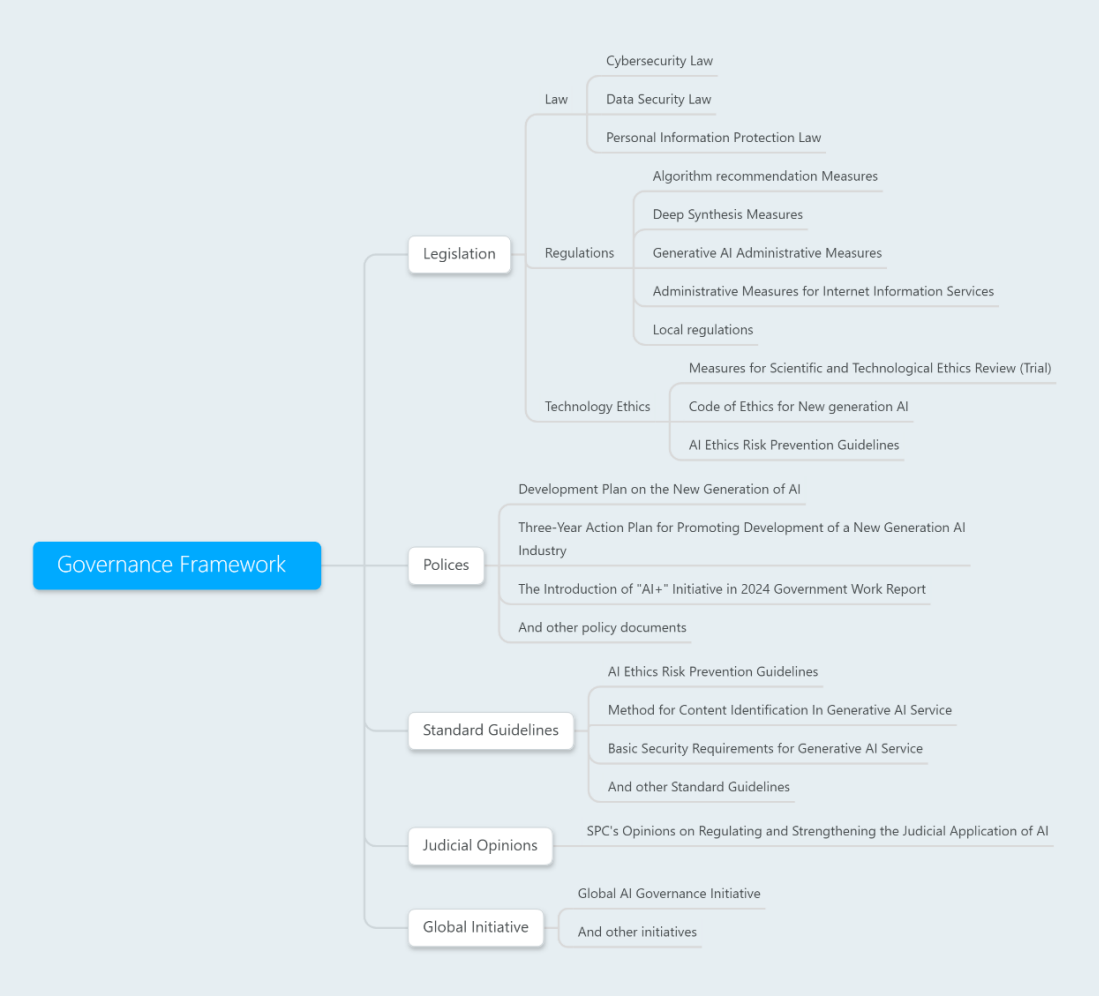
  - Safeguard national security and public interest: Protecting citizens and maintaining national security

China's structural strengths in AI

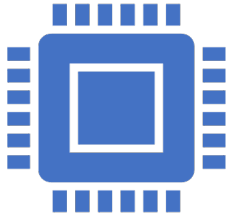
- Abundance of data (1.4 billion citizens)
- Data collected on a massive scale by the State
- Rare earths (1st reserves in the world and 40 times more than the US)
- Patents on AI (1st applicant according to WIPO in 2024)
- Scientific publications on AI (31% of world volume)
- Political commitment to AI and a Chinese AI market with structural barriers to entry (Chinese data, etc.)
- State funding and financial resources for companies

China’s AI legal framework is structured across 5 pillars:

Legislation
Policies
Standard Guidelines
Judicial Opinions
Global Initiatives



Key Regulations



Algorithm Recommendation Regulation:

Regulates how algorithms suggest content and services.

Came into force on March 1, 2022

Key Provisions:

- Transparency: Service providers must disclose the principles and objectives of their algorithms.
- User Rights: Users must be informed about the use of algorithms and have the option to disable algorithm recommendations.
- Content Management: Algorithms must not be used to spread illegal content or engage in illegal activities

Impact:

- Enhances transparency and user control over algorithmic decisions.
- Aims to prevent misuse of algorithms for harmful purposes

Deep Synthesis Regulation:

Covers technologies that create synthetic media and content.

Effective from January 10, 2023

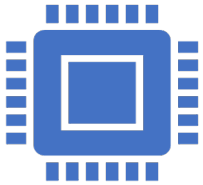
Key Provisions:

- Definition: Covers technologies that generate or edit text, images, audio, video, and virtual scenes using AI
- Consent: Providers must obtain explicit consent from individuals whose biometric information is edited.
- Labeling: Synthetic content must be clearly labeled to distinguish it from real content

Impact:

- Aims to prevent misuse of deep synthesis technologies for deception or harm
- Ensures transparency and protection of personal information

Key Regulations



Generative AI Regulation:

Governs the development and use of generative AI technologies.

Implemented on August 15, 2023

Key Provisions:

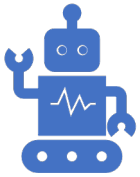
- Content Safety: Generative AI must not produce content that violates laws or public order.

- Data Security: Providers must ensure the security of data used and generated by AI systems.

- Ethical Standards: Generative AI must adhere to ethical guidelines and promote positive societal impact

Impact:

- Regulates the creation of AI-generated content to ensure safety and ethical use.
- Supports the development of responsible AI technologies



AI Labelling Measures:

Regulates mandatory labelling.

Taking effect on September 1, 2025

Key Provisions:

- Service providers: Explicit labels must be added to content generated or synthesized using AI technologies
- Internet application distribution platforms: must request explanation of whether service providers offer generative AI services and check materials related to the labeling.
- Users who use online information content transmission services to publish generated synthetic content must proactively declare it and use the labeling functions

Impact:

- Targeted to put an end to the misuse of AI generative technologies and the spread of false information.

Ethical Principles

- People-centered approach: AI development should prioritize human welfare and societal benefits.
- Respect for personal freedom and dignity: Ensuring AI respects individual rights and freedoms.
- Promotion of public well-being: AI should contribute positively to society and enhance quality of life
- Prevention and control of ethical risks: Developers, providers, and users must manage potential ethical issues and risks

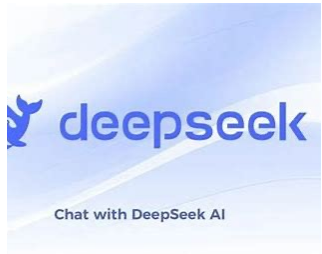
Compliance Obligations

- Obligations for service providers, technical supporters, and users: Defines responsibilities for all parties involved in AI.
- Protection of national and social security: Ensures AI applications do not compromise security.
- Requirements for ethical review of AI technologies: Mandates ethical assessments for AI projects
- Intellectual property protections for AI-generated content: Safeguards rights for content created by AI

Some hot topics…

AI generarated contents: who owns the rights ?

Social credit: progress or threat ?



Deepseek: a threat to protection of personal data ?

What's next ?

Global Initiatives

- Global AI Governance Initiative
- China and France's Joint Declaration on AI and Global Governance
- AI Capacity-Building Action Plan for Good and for All

Future regulatory trends

- From September 1, 2025, new 'Labeling Rules' will come into effect
- Ethical rules

Emerging regulations

- Official AI Law
- National standards on data annotation, pre-training and fine-tuning data, security emergency response guidelines, and security requirements.

Two Sessions (两会)

- major focus, reflecting China's commitment to becoming a global leader
- China's strategic focus on AI as a critical driver of economic and technological growth

THANK YOU

United States of America

US REGULATORY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE

Alan Greenfield
Shareholder
Greenberg Traurig, LLP
alan.greenfield@gtlaw.com

How the US has addressed AI: Applying IP laws

Patent Law & AI-Generated Inventions

- The U.S. Patent and Trademark Office (USPTO) has ruled that AI cannot be listed as an inventor on patents. In *Thaler v. Vidal* (2022), the U.S. Court of Appeals for the Federal Circuit upheld that under current law, only humans can be inventors.
- However, AI-assisted inventions (where a human is involved in the inventive process) may still be patentable

Trademark Law & AI

- AI-related trademarks follow standard trademark law, but AI is being used to help assess trademark applications and detect potential infringements.
- Some concerns exist about AI-generated branding or fake trademarks, but current laws generally treat AI-related trademarks similarly to traditional ones.

How the US has addressed AI: Applying IP laws

Copyright Law & AI-Generated Works

- The U.S. Copyright Office has stated that works created entirely by AI are not copyrightable because copyright law requires human authorship.
- However, works that involve AI as a tool but have substantial human input may be eligible for copyright protection. The Copyright Office evaluates applications on a case-by-case basis.
- In 2023, the Office issued guidance clarifying that if AI-generated content is mixed with human-authored elements, only the human-created portions qualify for copyright.

Trade Secret Protection

- AI models and algorithms are often protected as trade secrets, especially given the challenges of patenting software innovations.
- Companies like OpenAI and Google protect their AI models and datasets through trade secret laws, contracts, and cybersecurity measures.

How the US has addressed AI: New AI-focused laws and regulations

Version 1: Sectoral AI Laws

Version 2: Modern Privacy Laws

Version 3: Comprehensive AI Laws

Sectoral AI Laws

Chatbot Related AI Laws: California Section 17941

- Prohibits use of a bot to communicate or interact with another person online if it intends to mislead the person about its artificial identity for the purpose of deceiving the person and:
  - Incentivize the purchase or sale of goods in a commercial transaction, or
  - To influence a vote in an election
- Requires a "clear, conspicuous, and reasonably designed" disclosure to inform persons with whom the bot interacts/communicates
- A business is not liable under this section if it makes the disclosure

Chatbot Related AI Laws: Utah's AI Law S.B. 149

Non-Regulated Occupations Disclosures

- Applies if the business uses GenAI to interact with an individual in connection with commercial activities regulated by Utah's Division of Consumer Protection.
- If the individual interacting with the GenAI prompts or asks the GenAI to disclose whether he or she is interacting with a human.
  - Must clearly and conspicuously disclose to the individual that he or she is interacting with GenAI and not a human.

Regulated Occupations Disclosures

- If the person is using GenAI in providing the services of a "regulated occupation," the business must prominently disclose that the individual is interacting with GenAI.
- This applies regardless of whether the individual interacting with the GenAI has asked the GenAI if he or she is interacting with a human.

Sectoral AI Laws

HR Related AI Laws: Illinois Human Rights Act

- It is a civil rights violation for an employer to…
  - Use AI that subjects employees to discrimination, and
  - Fail to provide notice to an employee that the employer uses AI to recruit, hire, promote, terminate, discipline, etc.
    - If the employer does not give notice, then the employer may be subject to an investigation giving the employer 30 days to correct the violation.

HR Related AI Laws: New York City Law on Automated Employment Decision Tools (AEDT)

- AEDT means any form of AI that issues an output such as a score or recommendation that is used to substantially assist employment decisions.
- An employer can only use an AEDT to make an employment decision if:
  - The tool has undergone a bias audit (i.e., assessment of the tool's disparate impact), and the results have been posted and made publicly available.
  - The employer has provided notice that it uses such a tool.

Insurance Related AI Laws: Colorado S.B. 21-169

- Regulators are concerned with insurers using algorithms and predictive models as they may have a negative impact on the availability and affordability of insurance.
- The law prohibits the use of unfair discrimination based on protected classes and the use of AI that results in such discrimination.

Sectoral AI Laws – Other California Laws

California AI Transparency Act

- Requires a business that creates GenAI to implement disclosures, an AI detection tool, and contractual requirements that licensees will abide by the disclosure requirements.

California Healthcare Services: AI Act

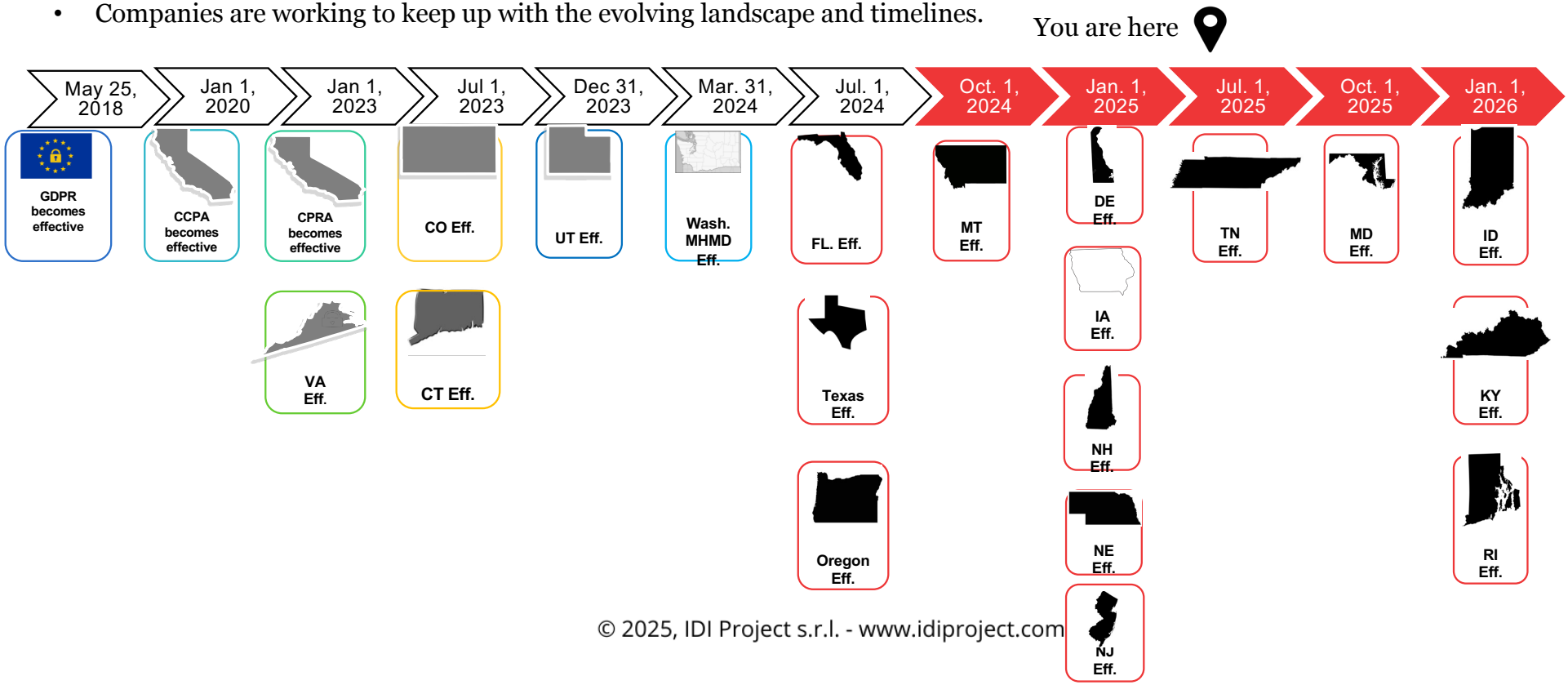
- Requires healthcare organizations that use GenAI to communicate with patients regarding clinical information to make sure the communications have certain disclosures.

California Generative AI: Training Data Transparency Act

- Requires developers (and deployers that become developers) of GenAI to post a “high level” summary of the training data used.

Modern Privacy Laws

- In the past four years, at least six states have passed comprehensive privacy laws
- At least thirteen more states will go online in the next two years
- Companies are working to keep up with the evolving landscape and timelines.



Comprehensive AI Laws

The Colorado AI Act (CAIA)

- Enacted May 2024
- Goes into effect February 1, 2026
- Arguably first comprehensive AI Act in the United States
- The CAIA is primarily focused on **high-risk artificial intelligence systems**, which is defined as any system that, when deployed, makes — or is a substantial factor in making — a "consequential decision."

CAIA – High-Risk Systems Comparison

CO v. EU: High-Risk Systems

Colorado	EU
Education	Education
Employment	Employment
Essential government service	Essential public/private services
Financial or lending service	*(includes certain financial services)*
Health care services	*(includes certain healthcare)*
Insurance	*(includes certain insurance)*
Legal services	
Housing	
	Immigration and border control
	Justice and democratic process
	Biometrics
	Critical infrastructure management
	Law enforcement

CAIA - Key Points

- The CAIA is designed to protect against **algorithmic discrimination**, namely unlawful differential treatment that disfavors an individual or group on the basis of protected characteristics.

- The law imposes various obligations relating to documentation, disclosures, risk analysis and mitigation, governance, and impact assessments for **developers** and **deployers** of high-risk AI systems. These disclosures include:
  - Deployers must clearly and readily make available on their website:
  - The type of high-risk AI systems that are currently deployed.
  - How they manage known or reasonably foreseeable risks of algorithmic discrimination that may arise.
  - The nature, source, and extent of the information collected and used by the deployer in connection with the AI system.

- With respect to ***all*** AI systems that interact with consumers, deployers must ensure that consumers (even if not high-risk) are aware they are interacting with an AI system, unless it would be obvious to a reasonable person.

- The state attorney general can bring an action for violations of the CAIA as an unfair or deceptive trade practice; there is **no private right of action** available.

CAIA – Deployer Responsibilities

Notification to Consumers

- Deployers must notify consumers when they have deployed a high-risk AI system to make — or to be a substantial factor in making — a consequential decision about the consumer before the decision is made. This disclosure must include:
- A description of the high-risk AI system and its purpose.
- The nature of the consequential decision.
- Contact information for the deployer.
- Instructions on how to access the required website disclosure (see below for more).
- Information regarding the consumer's right to opt out of the processing of the consumer's personal data for profiling.

Handling Adverse Decisions

- Where a high-risk AI system reaches a decision that is adverse to the consumer, the deployer must provide the consumer with a statement regarding:
- The reason for the consequential decision.
- The degree to which the high-risk AI system contributed to the decision.
- The type of data that was processed by the system and the sources of that data.
- The consumer must be given the opportunity to correct any incorrect personal data used as well as an opportunity to appeal the adverse decision and request human review.

THANK YOU

Brazil

BRAZILIAN REGULATORY FRAMEWORK FOR ARTIFICIAL INTELLIGENCE

Luciana Gonçalves Bassani
luciana.bassani@gameleirapelagio.com.br
Corporate and Comercial Lawyer
IDI Country Expert on Franchising
Gameleira, Pelagio, Fabião e Bassani Sociedade de Advogados

I – Introduction

- In **December 2024**, the **Federal Senate** approved **Bill No. 2,338/2023** ("AI Bill"), which is currently under review in the **Chamber of Deputies**;

- On **April 4th**, a **Special** Committee was established, to analyze the AI Bill and several related AI Bills;

- **Similarities with EU AI Regulation**.

Foto: https://latinexclusive.com/pt-br/magazine/48h-rio-de-janeiro

II – Bill No. 303/2024: Industrial Property for AI System

The Bill aims to amend Article 6 of Brazilian Industrial Property Law, stipulating that when an **AI system autonomously generates an invention, a patent may be filed on its behalf**. In such cases, the AI system would be recognized as the **inventor** and **rights holder** of the invention.

Currently, the Bill is **under review** in the Chamber of Deputies and **has not yet been put to a vote.**

Since this subject has not yet been regulated, Brazil's **National Institute of Industrial Property (INPI)** clarified its position in 2022 through **Ordinance No. 24/2022**, deciding that an **AI system cannot be a patent inventor,** as **Article 6 of Brazilian Industrial Property Law** reserves this right solely to a **natural person.**

Current **Brazilian legislation** does **not regulate copyright protection** for **AI systems** and there is **no legislative proposals** before the **National Congress** (Brazilian Parliament) addressing this matter.

Although **AI Bill** regulates various **aspects of AI system**, it does **not** clearly **define authorship rules** for **AI-generated works**, creating a **legislative gap**.

However, AI Bill establishes:

- AI agents are subject to **Brazilian Copyrighted Law** concerning **licensing** and **remunaration of authors** (Art. 65);
- **AI developer** must **disclose copyrighted content** used and **safeguard secrets** (Art. 62); and
- **Author** have the **right to prohibit the use of their works**, subject to material and moral damage if violated, even during development (Art. 64).

.

III – Bill No. 2,338/2023 ("AI Bill"): Definitions

- **AI System**: based on a **machine that infers**, from a set of **data** or information it **receives**, how to **generate results**, in particular **prediction**, **content**, **recommendation** or **decision** that **may influence** the **virtual**, **physical** or **real environment** (Art. 4, I);

- Bill classifies **AI agents** as **developers**, **distributors**, and **deployers** (as individuals or legal entities, whether public or private) that:

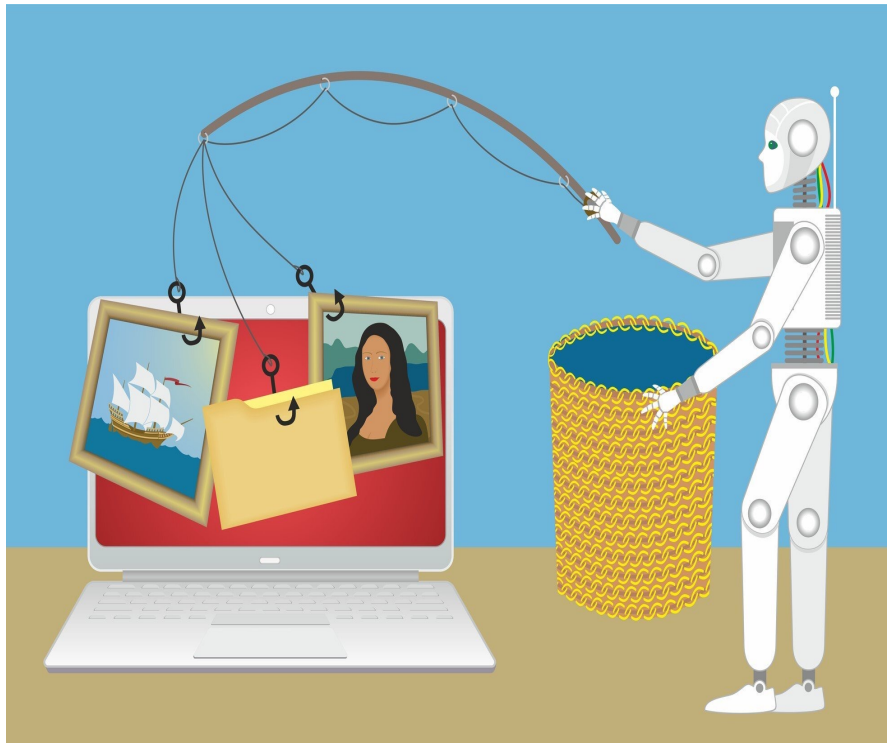


Photo: Eva Almqvist/iStock

- **Developers:** develop an AI system, with the intent to market or apply it for providing a service, under their own name or brand, whether receiving compensation or free of charge (Art. 4, V);

- **Distributors:** make available or distribute an AI system for third-party use, whether receiving compensation or free of charge (Art. 4, VI).

- **Deployers:** employ or use an AI system in their own name or for their benefit, including configuring, maintaining, or supporting its operation and monitoring through data provision (Art. 4, VII).

IV – Risk Categorization

- **Before the introduction** of an AI system **in the market**, the AI agent may **conduct a preliminary assessment** to **determine its risk level** (art. 12), in accordance with the criteria therein:

- **Excessive-Risk**: AI systems are **prohibited due to their excessive risk**, when its development, implementation and use may:

  - **cause significant harm to health, safety, or other fundamental rights**, even **inducing behaviors** or **exploiting vulnerabilities** (art. 13, I, a and b);

  - assess **personal characteristics**, or **past behavior** (criminal or otherwise) to evaluate **risks of criminal offenses** (art. 13, I, c),

  - develop systems for **remote real-time biometric identification** in **publicly accessible spaces**, among other scenarios outlined in the Bill (art. 13, IV).

- **<u>High-Risk Systems</u>:** considers the **likelihood and severity of adverse impacts** on affected individuals or groups (Art. 14), such as:

  - **candidate recruitment** and **evaluation** and decisions on **performance**, **promotions or termination of employment relationships** (Art. 14, III);

  - **autonomous vehicles** in **public spaces**, which may pose **significant risk** to **physical safety** (Art. 14, VII);

  - **support in medical diagnostics** and procedures with **significant risk** to **physical** and **mental well-being** (Art. 14, VIII);

  - **biometric identification** and authentication **for emotion recognition**, excluding biometric identity verification systems **(Art. 14, XI**), among other cases.

- **National AI Regulation and Governance System ("SIA")** will be **responsible for regulate the classification of the high-risk AI systems** and identify **new** high-risk application scenarios.

- To promote national technological development, **SIA will regulate simplified regimes** involving regulatory obligation **flexibilities** for encouraging **innovation and scientific and technological research** (Arts. 1, §2 and 4, XVIII – regulatory sandbox).

V – Liability

- **Liability for damages** caused by AI systems remains subject to (i) the **rules of liability under the Civil Code** (CC), **based on fault** (subjective liability) and (ii) the **End Consumer Defense Code** (CDC) when occurring within consumer relations (Arts. 35 and 36); **strict liability**, regardless of proof of fault or intent (merely proof of a causal link and inversion of burden of proof);

- Article 927, sole paragraph, of the CC, determines that the agent **shall be strictly liable for damage caused**, when the activity normally performed **involves risk** to third parties.

- AI Agents are also subject to liabilities established by:

  - **LGPD (Brazilian GDPR)**, when **processing personal** data during the **development**, **implementation**, and **use** of AI system (Art. 1º, §1º, I, Art. 22, Art. 27, Art. 30 IV).

  - The **Brazilian National Environmental Policy Act,** based on **strict liability** (Art. 1, §1, III).

V – Sanctions

- Bill provides for **administrative sanctions** against AI agents who commit violations, including: (i) **warnings**; (ii) partial or complete, **temporary or permanent suspension of AI system** development; supply, or operation; (iii) and **standard fines up to R$50,000,000.00** (fifty million reais) **per violation** or, for private legal entities, **up to 2% of their gross revenue**, their **group's** gross revenue in Brazil for the last fiscal year, **excluding taxes** (Art. 50).

- Sanctions shall be imposed following **administrative proceedings** with **full right of defense**, applied progressively, according to case specifics and considering criteria, such as (Art. 50, §1):

- **Severity** of the **violation** and **rights infringement**;
- Violator's **good faith**;
- **Gained** or **intended advantage**;
- Violator's **economic condition**;
- Repeated **offenses**;
- **Degree** of **harm**;
- Violator's **cooperation**;
- Repeated **internal risk mitigation measures** (e.g., **ethics codes** and **algorithmic impact assessments**);
- Adoption of **good practice** and **governance policies**;
- Prompt **corrective actions**;
- **Proportionality** between **violation severity** and **sanction intensity**; and
- **Cumulation** with other **sanctions** already applied for the **same act**.

- For development, supply, or use of **high-risk AI systems**, sanctions shall include at least a fine and, for legal entities, **partial or complete, provisional or permanent suspension** of activities (Art. 50, §4).

THANK YOU! OBRIGADA!

Canada‘s Emerging Framework for AI and Data Regulation

Peter Snell

Partner, Franchise Group

Cassels, Brock & Blackwell LLP

psnell@cassels.com

Canada‘s Emerging AI Regulatory Framework

- **Bill C-27 (*Digital Charter Implementation Act*) introduces:**
  - *CPPA* – Privacy modernization
  - *AIDA* – Regulation of high-impact AI
  - *PIDPTA* – Enforcement mechanism
- **Goals:**
  - Balance innovation with oversight, transparency and harm prevention
  - Strengthen data rights
- **Provincial efforts:** Quebec, Ontario and Alberta

Artificial Intelligence and Data Act (AIDA)

- Applies to high-impact AI systems with potential for harm to individuals, property or the economy
- **Developer/provider/user obligations:**
  - Transparency, accountability, risk mitigation
- Criminal penalties for reckless/malicious use
- Establishes AI and Data Commissioner for regulation and enforcement

Consumer Privacy Protection Act (CPPA)

- **Expands inidividual rights:**
  - Data portability
  - Right to deletion
  - Enhanced consent
- **Enforcement powers:**
  - Binding orders by Privacy Commissioner
  - Fines – up to $25 million or 5% of global revenue
- Aligned with AIDA to refulate both data and AI systems

Transparency & Sector-Specific Developments

- **AIDA mandates:**
  - Disclosure of AI use
  - Human oversight in decisions
  - Prevention of deception & harm
- **Provincial laws:**
  - Quebec Law 25: Right to know & challenge automated decisions
  - Ontario: Public-sector hiring disclosure
  - Alberta: 1-year data retention for AI-based decisions
- **Federal Code of Practice for Generative AI:**
  - Voluntary principles – Fairness, safety, transparency, oversight
  - Builds path to AIDA compliance

Implications for Businesses and Franchise Systems

- **Preparation Steps:**
  - Identify high-impact AI systems
  - Ensure transparency in customer/franchisee interactions
  - Implement bias & risk mitigation frameworks
  - Review contracts (data ownership, oversight, compliance)
  - Align with Code of Practice for Generative AI & applicable legislation
- **Franchise systems focus:**
  - Deploy explainable, privacy-conscious AI
  - Strengthen trust and reduce regulatory risk

Thank you!

Chile

No specific, unique and comprehensive regulation that governs A.I., but several pieces of legislation to establish a legal framework.

- **Law 21.383 (2021):**
  - Amends the Constitution and establishes that the scientific and technological development will serve the people and will be carried out with respect to life and physical and mental integrity. It further establishes that Law will regulate the requirements, conditions and restrictions for its use, ensuring the protection of mental activity and the information arising from it.
- **Implementation of a National Public Policy on A.I. (2021 and on...)**
  - Main goal of this Public Policy: the creation and attaction of talent, procurement of data and infraestructure, promotion of R&D in the field and establishment of the basic ethical and legal rules to position Chile as a key actor in A.I. in the Latin American region.

Chile

- **Draft of Law on Artificial Intelligence (currently pending in Congress since 2023).**

  Inspired on the European A.I. Act.

  - Creates the National Commission on Artificial Intelligence.
  - Establishes an evaluation and autorization process for all I.A. Systems.
  - Qualification of certain A.I.systems as “high risk”and the requirements needed to de development, distribution, commercialization and use of A.I., including compliance of human monitoring principle.
  - Forbids all A.I. Systems that are qualified as unacceptable “high risk”.
  - Establishes Universal requirements for all A.I. Systems, as to transparency and information.
  - Implements an Authorized A.I. Systems Register.
  - Establishes sanctions for developers, providers and users that infringe the regulations of this Law.

Chile

- **Other local regulations with impact in A.I.**
  - Private Life Protection Act (Law 19.628 dated August 1999, last updated in 2022). This regulation will be replaced, as from December 1st 2026, by Law 21.719, which Regulates the Protection and Treatment of Personal Data and creates the Personal Data Protection Agency, with the purpose to update Chilean Law in this field in accordance with current international regulations and particularly E.U.'s GDPR.
  - Chilean Constitution (establishes data protection as a right and provides that scientific and technological development shall serve the people) dated 1980 and last updated in 2024.
  - Intellectual Property Law (dated 1970, last updated in 2017).
  - Industrial Property Law (dated 2006, last updated in 2022).
  - Civil Code (dated 1885/2006, last updated in 2024).
- **What is the picture today?**

Thank you for your attention