The “One Big Beautiful” Bill and the State of AI Regulation

July 31, 2025
By Albena Petrakov

After several weeks of back and forth on a potential 10-year moratorium on state or local AI legislation and regulation enforcement, the final version of the so-called One Big Beautiful Bill Act, signed into law on July 4, 2025 (Pub. L. No. 119-21), abandoned the proposed provision. Accordingly, companies must be alert to and comply with a variety of evolving state and local laws governing the use and deployment of AI tools. In addition, companies that supply AI systems or produce outputs intended for use in the EU are subject to the EU AI Act. Here we will provide a high-level overview of the state laws that are AI-specific (as opposed to regulating use cases or general conduct that might involve AI).

Colorado AI Act
The Colorado AI Act is scheduled to go into effect on February 1, 2026. It is considered a consumer protection law and imposes obligations on developers and deployers of so-called "high-risk" AI systems "to use reasonable care to avoid algorithmic discrimination in the high-risk system." The law creates a rebuttable presumption that a developer or deployer used reasonable care if they complied with specified provisions in the law.

Texas Responsible Artificial Intelligence Governance Act
The Texas governor recently signed the Texas Responsible Artificial Intelligence Governance Act, which will become effective on January 1, 2026. It creates a regulatory system for AI development and use, AI disclosure requirements for government agencies, a program that allows AI development with relaxed legal constraints, and an advisory council to analyze AI use and provide recommendations to state agencies. Although it primarily regulates governmental agencies and health care providers, the new law is of relevance to private sector organizations, more generally the new law clarifies that:

It is unlawful for any person to use an AI system to intentionally discriminate against individuals based on a protected characteristic, with limited exceptions for certain insurance companies and financial institutions.

Showing a disparate impact on a given group is insufficient to demonstrate intentional discrimination.

Maine Chatbot Disclosure Law
On June 12, 2025, Maine enacted H.P. 1154, a law requiring disclosure of the use of AI chatbots. Under the law, a person may not use an AI chatbot of any other computer technology to engage in trade and commerce with a consumer in a manner that may mislead or deceive a reasonable consumer to believing that the consumer is engaging with a human being, unless the consumer is notified in a clear and conspicuous manner that the consumer is not engaging with a human being. Violation of the law is a violation of the Maine Unfair Trade Practices Act.

New York RAISE Act
New York state lawmakers passed the groundbreaking *Responsible AI Safety and Education Act* (RAISE Act) on June 12,

2025. New York will become the first state to impose enforceable AI safety standards on powerful “frontier models” to prevent catastrophic harm by advanced models, if the governor signs off. The law would take effect 90 days after the governor signs the bill.

The law applies to AI models with $100M+ compute cost (or $5M+ for certain “distilled” versions) and covers any frontier models developed, deployed, or operated in New York

The law imposes on developers, of extremely large-scale AI systems, sweeping transparency and safety obligations. They must develop a safety and security protocol and publish the safety protocols (with limited redactions for trade secrets or security purposes). Any serious incident indicating heightened risk must be reported to state regulators within 72 hours. Businesses must participate in ongoing reassessment of protocols as models evolve.

Utah Artificial Intelligence Consumer Protection Amendments
On March 27, 2025, Utah Governor Spencer Cox signed S.B. 226, a law governing the use of GenAI in consumer transactions and regulated services. The law:

- States it is not a defense to violation of any law administered by the State Division of Consumer Protection that AI:
  - made the violative statement,
  - undertook the violative act, or
  - was used in the furtherance of the violation.
- Requires disclosure for the use of GenAI when:
  - in connection with a consumer transaction, and
  - providing services in a regulated occupation.
- Establishes a safe harbor for clear and conspicuous disclosure GenAI is used, subject to additional rulemaking specifying forms and methods of disclosure.
- Allows the Division of Consumer Protection to impose administrative fines of up to $2,500 per violation.
- Gives courts the power to:
  - declare an act or practice violates the law,
  - issue an injunction for violation,
  - order disgorgement of money received in violation,
  - impose fines of up to $2,500 per violation, plus costs and fees.

The law is effective May 7, 2025.

EU AI Act
The EU AI Act, known as Regulation (EU) 2024/1689, is a comprehensive regulatory framework designed to govern AI systems and the organizations that supply and use them within the EU. It categorizes AI systems based on their risk levels and imposes obligations on providers, importers, distributors, and deployers of AI systems.

Compliance deadlines vary, with most provisions applying from August 2, 2026, but some have earlier compliance dates, including:

- Prohibited AI practices are banned outright from February 2, 2025[1],
- AI literacy[2] obligations apply from February 2, 2025,

- GPAI model rules become effective on August 2, 2025, and
- Penalties, which apply from August 2, 2025, except penalties applicable to GPAI model providers, which apply from August 2, 2026.

Rules on high-risk AI systems forming the safety components of products covered by existing EU product safety legislation apply from August 2, 2027.

The EU AI Act defines AI systems as machine-based systems designed to operate with varying levels of autonomy and adaptiveness, generating outputs such as predictions, content, recommendations, or decisions that can influence environments. It excludes certain AI systems used for military, defense, national security, and other specific purposes.

Organizations must determine their role in the AI supply chain, whether as providers, deployers, distributors, or importers, and comply with the corresponding obligations.

- Providers must create technical documentation, conduct conformity assessments, and appoint authorized representatives, among other requirements.
- Deployers must ensure human oversight, monitor AI system performance, and complete fundamental rights impact assessments, if applicable.
- Distributors must verify compliance with CE marking and conformity declarations and take corrective actions if necessary.
- Organizations must assess whether their AI systems are high-risk and meet technical requirements, including risk management systems and data governance practices

In connection with the upcoming effective date for the general-purpose AI, the European Commission issued guidelines for providers to assess whether their model is a general-purpose AI model.

Article 3(63) AI Act defines a 'general-purpose AI model' as *'an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, 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, except AI models that are used for research, development or prototyping activities before they are placed on the market'*. This definition lists, in a general manner, factors that determine whether a model is a general-purpose AI model. Nevertheless, it does not set out specific criteria that potential providers can use to assess whether a model is a general purpose AI model.

The specific criteria the commission chose is based on computational power. An indicative criterion for a model to be considered a general-purpose AI model is that its training compute is greater than 1023 FLOP and it can generate language (whether in the form of text2 or audio3), text-to-image or text-to-video. If a general-purpose AI model meets the latter criteria, but does not display significant generality or is not capable of competently performing a wide range of distinct tasks, it is not a general-purpose AI model. Similarly, if a general-purpose AI model does not meet that criterion but, exceptionally, displays significant generality and is capable of competently performing a wide range of distinct tasks, it is a general-purpose AI model.

In Conclusion
Companies must create a risk-management framework to navigate a complex, evolving patchwork of rules. With compliance deadlines stretching across 2025–2027, organizations must now proactively monitor and adapt to both U.S. mosaic regulation and EU mandates depending on their markets and use cases.

Ultimately, treating AI regulation as a dynamic and strategic compliance horizon will be essential to manage legal risk, maintain trust, and sustain innovation in this rapidly evolving landscape.

[1] Prohibited AI practices include:

- Subliminal techniques which can materially distort a person's behavior by impairing their ability to make an informed decision in a way that causes or is reasonably likely to cause them significant harm.
- Exploiting the vulnerabilities of a person or specific groups of people (for example, due to their age, a disability or economic situation) which can materially distort their behavior in a way that causes or is reasonably likely to cause them significant harm.
- Social scoring systems based on known, inferred or predicted personality characteristics which causes detrimental or unfavorable treatment that is disproportionate or used in a context unrelated to the context in which the data was originally collected.
- Risk assessment systems which assess the risk of a person to commit a crime or re-offend (except in support of a human assessment based on verifiable facts).
- Indiscriminate web-scraping for the purposes of creating or enhancing facial recognition databases.
- Emotion recognition systems in the workplace or educational institutions (except for medical or safety reasons).
- Biometric categorization systems used to infer characteristics, such as race, political opinions or religion.
- Real-time, remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement except (subject to safeguards and within narrow exclusions) searching for victims of abduction, preservation of life and finding suspects of certain criminal activities (as listed in *Annex II: criminal offences permitting use of real-time biometric systems*). Real time means live or near-live material, to avoid short recording delays circumventing the prohibition.

[2] AI literacy is defined as the skills, knowledge and understanding of a deployer or a provider (and other affected persons) to make informed use of AI systems and to be aware of both the opportunities of AI systems and the risks of potential harm. The obligation to take measures to ensure a sufficient level of AI literacy is set out in Article 4.