



June 01, 2026

# Connecticut Enacts Comprehensive AI Regulation — What Businesses Need to Know

New legislation positions Connecticut at the forefront of AI regulation

## At a Glance

- The Connecticut Artificial Intelligence Responsibility and Transparency Act targets high-risk and employment-related systems and is scheduled to take effect starting October 1, 2026.
- Companies must implement governance programs, risk assessments, and clear disclosures — not just legal review.

On May 27, 2026, Connecticut Governor Ned Lamont signed Public Act No. 26-15/SB 5, referred to as the Connecticut Artificial Intelligence Responsibility and Transparency Act (the Act) into law. The Act, passed by the Connecticut legislature on May 1, 2026, addresses AI across a broad range of domains, including high-risk AI systems, frontier model development, employment-related AI tools, AI companions, generative AI content provenance, and a regulatory sandbox. Companies developing, deploying, or using AI technologies in connection with Connecticut businesses and residents should begin assessing their compliance obligations now, as certain provisions take effect as early as October 1, 2026, with others phasing in through October 1, 2027.

## AI-Related Provisions Taking Effect in 2026

### High-Risk AI Systems (Effective October 1, 2026)

The Act's most broadly applicable provisions impose a reasonable care standard on developers, integrators, and

deployers of “high-risk AI systems” — systems intended to make or be a substantial factor in making “consequential decisions” affecting employment, education, financial services, housing, insurance, legal services, or access to essential government or health care services. Developers must furnish deployers with documentation on intended uses, training data, discrimination risks, bias mitigation measures, and human monitoring protocols, and must publicly disclose the types of high-risk systems they offer. If a developer discovers that a system has caused or is reasonably likely to have caused algorithmic discrimination affecting at least 1,000 consumers, it must notify the attorney general and all known deployers within 90 days. Integrators must contract with developers to allocate compliance obligations. Deployers must implement risk management programs, complete impact assessments before deployment and annually thereafter, retain assessments for at least three years, and notify consumers before the system contributes to a consequential decision — including providing enhanced disclosures and appeal rights for adverse decisions.

## AI Subscription Disclosures (Effective October 1, 2026)

Subscription-based AI providers must furnish consumers with written pre-contract disclosures of key terms, including usage limitations and any discretion to reduce functionality. Consumers must provide written acceptance before the provider may collect fees. Renewal disclosures are required for any new limitations.

## Frontier Model Developers: Whistleblower Protections (Effective October 1, 2026)

The Act protects employees of “frontier developers” — persons doing business in Connecticut who train foundation models using at least 10<sup>26</sup> operations — from retaliation for reporting catastrophic risks, defined as foreseeable risks of death or serious injury to 50+ individuals or \$1 billion+ in property damage linked to CBRN weapons or autonomous cyberattacks. Large frontier developers (annual gross revenue exceeding \$500 million) must establish anonymous internal reporting processes by January 1, 2027. Violations carry civil penalties of up to \$1,000 per violation, enforceable by the attorney general.

## WARN Act Disclosure (Effective October 1, 2026)

Employers filing WARN Act notices must disclose whether layoffs are related to AI or other technological changes.

## AI-Related Provisions Taking Effect in 2027

### AI Companions (Effective January 1, 2027)

The Act broadly defines “AI companion” as any AI model that communicates in natural language and simulates human conversation through text, audio, or video — a definition that sweeps in most general-purpose consumer chatbots. Operators must implement protocols to detect expressions of suicide, self-harm, or imminent violence and refer users to mental health resources. Operators must also disclose the AI’s nonhuman nature where a reasonable person could be misled. Heightened protections apply to users under 18, including prohibitions on encouraging self-harm, offering unauthorized mental health services, sexually explicit interactions, and manipulative engagement techniques. The attorney general enforces these protections under the Connecticut Unfair Trade Practices Act (CUTPA).

## Automated Employment Decision Technologies (Effective October 1,

2027)

The Act regulates any technology that processes personal data and produces an output — such as a score, rank, or recommendation — that is a substantial factor in employment-related decisions, encompassing hiring platforms, resume screeners, assessment tools, scheduling algorithms, and performance analytics. Deployers must provide pre-decision written notice identifying the tool, its purpose, data categories, and assessment methodology. For adverse decisions, deployers must disclose the degree of AI contribution and allow individuals to examine and correct their data. The Act amends the Connecticut Fair Employment Practices Act to clarify that use of such technology is not a defense to a discrimination complaint; however, courts and the Connecticut Commission on Human Rights and Opportunities may consider evidence of anti-bias testing as a mitigating factor, evaluating “the quality, efficacy, recency and scope of such testing or efforts, the results of such testing or efforts and the response thereto.” This is not a safe harbor, but employers who document rigorous bias-testing methodologies and corrective actions will be better positioned in enforcement proceedings.

## Generative AI Provenance and Watermarking (Effective October 1, 2027)

Generative AI systems with over one million monthly users must embed provenance data in AI-generated or materially altered audio, image, or video content, using commercially reasonable methods including standards established by the Coalition for Content Provenance and Authenticity. Exemptions apply to artistic and satirical content, text-only public interest content, B2B systems, and video games.

## Enforcement, Affirmative Defenses, and Bias Testing

The attorney general has exclusive enforcement authority under CUTPA for most provisions and does not create any new private rights of action. Furthermore, the Act clarifies that a private right of action, including under CUTPA, does not apply for violations related to (i) AI subscription disclosures (Section 1), (ii) AI companion safety protocols and disclosure for users 18 years of age or older (Section 5), (iii) automated employment-related decision technology (Section 8-11), and (iv) generative AI provenance data (Section 15).

The Act establishes a mandatory cure period from October 1, 2026, through September 30, 2027; thereafter, cure opportunities are discretionary. The Act creates a rebuttable presumption that a developer, integrator, or deployer used reasonable care if it complied with the Act’s requirements. An affirmative defense is available where the entity discovered the violation through red-teaming, cured it within 60 days with notice to the attorney general, and complied with the NIST AI Risk Management Framework, ISO/IEC 42001, or an equivalent framework. Notably, the definition of “algorithmic discrimination” expressly excludes systems used solely for bias testing, compliance testing, or efforts to expand applicant pools to increase diversity — ensuring that proactive testing efforts do not themselves create liability.

## Key Takeaways

Connecticut’s new AI law places the state among the most aggressively regulated jurisdictions for AI in the United States. Companies should promptly inventory AI systems that may qualify as high-risk or as automated employment decision technologies; review vendor and integrator contracts for compliance with the Act’s allocation requirements; build disclosure and notice frameworks in advance of the October 1, 2026, effective date; audit chatbot and companion products for compliance with the January 1, 2027, obligations; and document bias-testing methodologies, results, and corrective actions to position favorably under the Act’s anti-bias testing framework.

*The material contained in this communication is informational, general in nature and does not constitute legal advice. The material contained in this communication should not be relied upon or used without consulting a lawyer to consider your specific circumstances. This communication was published on the date specified and may not include any changes in the topics, laws, rules or regulations covered. Receipt of this communication does not establish an attorney-client relationship. In some jurisdictions, this communication may be considered attorney advertising.*

## Meet the Authors



**Mason S. Medeiros**  
Associate

Minneapolis  
+1 612 766 7352  
mason.medeiros@faegredrinker.com



**Joseph C. O'Keefe**  
Partner

New York  
+1 212 248 3274  
joseph.okeefe@faegredrinker.com

## Related Legal Services

Government & Regulatory  
Labor & Employment  
Litigation  
Privacy, Cybersecurity, Data Ethics & Strategy  
E-Discovery & Information Management  
State Attorneys General

## Related Sectors

Technology

## Related Topics

AI-X