Ogletree Deakins

Colorado's Artificial Intelligence Act: What Employers Need to Know

May 20, 2024

By Jennifer G. Betts, Danielle Ochs, and Michael H. Bell

On May 17, 2024, Colorado Governor Jared Polis signed into law Senate Bill (SB) 24-205, "Concerning Consumer Protections in Interactions With Artificial Intelligence Systems" (the "Colorado Artificial Intelligence (AI) Act"), a groundbreaking measure designed to regulate the private-sector use of AI systems, and, specifically, the risk of algorithmic discrimination arising from the use of high-risk AI systems. The law, which will take effect on February 1, 2026, will make Colorado the first U.S. state to enact comprehensive legislation regulating the use and development of AI systems.

When the governor signed SB 24-205, he expressed his hope and expectation that, before the effective date, there would be amendments to the law based on stakeholder engagement. As a result, the structure described below may be amended before the effective date and employers may want to monitor additional developments.

Quick Hits

- With Governor Jared Polis's signing into law SB 24-205, Colorado becomes the first U.S. state to enact comprehensive legislation regulating the use and development of AI systems.
- The law addresses, among other things, the risk of algorithmic discrimination "arising from the intended and contracted uses of … high-risk artificial intelligence system[s]."
- The Colorado AI Act will take effect on February 1, 2026.

Colorado's AI Act, SB 24-205, is designed to regulate the use of "high-risk" AI systems, imposing compliance obligations on both "developers" (i.e., creators) and "deployers" (i.e., users) of AI systems. Structurally, the law is similar to the European Union's recently adopted Artificial Intelligence Act. The Colorado AI Act will become part of Colorado's Consumer Protection Act. While the Colorado AI Act does not appear to authorize private rights of action (providing the Colorado attorney general with exclusive enforcement authority), there is some ambiguity regarding enforcement, as the legislation also provides that a violation of the act will be a deceptive trade practice under Colorado's Consumer Protection Act—which law *does* allow for private rights of action.

What Employers Need to Know

Colorado's AI Act contains different requirements and rules depending on whether an entity is a developer or a deployer. Because the employer community will largely fall into the "deployer" definition, this article highlights aspects of the law that are most pertinent to deployers/employers using AI as part of their people practices.

Colorado Employers Using Certain AI Systems Will Be Subject to the Law

The Colorado AI Act is designed to cover the employment context. Specifically, it is intended to address the use by any persons or entities in Colorado of AI systems in employment decisions and to protect any "consumers," defined as Colorado residents. The framework provides a narrow exemption for employers with fewer than fifty employees that do not use their own data to train or further improve their AI systems.

Colorado Has Developed Its Own "Algorithmic Discrimination" Definition

The Colorado AI Act defines "algorithmic discrimination" to mean any condition in which the use of an AI system "results in an unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, veteran status, or other classification protected under the laws of [Colorado] or federal law."

High-Risk AI Systems Are in the Crosshairs

As AI laws continue to be proposed, developed, and implemented throughout the world, employers are continually facing evolving and different definitions of what qualifies as a covered AI system. Colorado's AI Act is focused on "high-risk" AI systems, defined as any AI system that "makes, or is a *substantial factor* in making, a *consequential decision*." (Emphasis added.) Importantly, a "consequential decision"—i.e., "a decision that has a material legal or similarly significant effect" on the provision or denial to Colorado residents of a broad array of essential services, opportunities, and entitlements—includes a decision related to "employment or an employment opportunity." A "substantial factor" means one that (1) "assists in making a consequential decision"; (2) "is capable of altering the outcome of a consequential decision"; *and* (3) "is generated by an artificial intelligence system." "'Substantial factor' includes any use of an artificial intelligence system to generate any content, decision, prediction, or recommendation concerning a consumer that is used as a basis to make a consequential decision concerning the consumer." There are also certain enumerated exclusions from the definition of high-risk AI systems. The current definitions leave much room for ambiguity that will hopefully be the source of refinement in future guidance.

Various New Obligations Will Exist for Deployers/Employers

Under the Colorado AI Act, deployers/employers are required to use "reasonable care" to protect consumers from any "known or reasonably foreseeable risks of algorithmic discrimination." The law creates a rebuttable presumption of reasonable care if certain compliance steps are taken, including:

a. *Risk-management policies and programs*. Deployers/employers must implement a risk management policy and program meeting certain defined criteria. This risk management policy and program must be an "iterative process" that is regularly and systematically reviewed and updated. Further, the risk management

policy and program must be reasonable in consideration of various listed factors, including: risk management frameworks published by the Colorado attorney general or guidance and standards issued by various identified national or international risk management frameworks for AI (such as the "Artificial Intelligence Risk Management Framework" published by the National Institute of Standards and Technology (NIST)); the size and complexity of the deployer/employer; and the nature and scope of the high-risk AI system used by the deployer/employer.

b. *Impact assessments*. Covered employers must also complete annual impact assessments for high-risk AI systems (or even more frequently if there is an intentional and substantial modification of the system). These impact assessments are similar to the annual bias audits required by New York City's AI law. Among other things, an impact assessment must include:

- a statement of the purpose, use cases, and benefits of the AI system;
- an analysis of whether there are "known or reasonably foreseeable" risks of algorithmic discrimination, and, if so, the steps taken to mitigate the risks;
- a description of the categories of data processed as inputs and the outputs of the AI system;
- if the system has been customized by the deployer/employer, "an overview of the categories of data … used to customize" the system;
- "metrics used to evaluate the performance and known limitations" of the AI system;
- a "description of any transparency measures taken concerning" the AI system, "including any measures taken" to notify Colorado consumers of the use of the system; and
- "a description of the post-deployment monitoring and user safeguards provided" relating to the AI system.

c. *Notices to consumers*. Colorado employers are also required to provide various notices. Among other provisions in Colorado's AI Act is one requiring consumers to be notified that a deployer/employer has deployed a covered AI system "to make, or be a substantial factor in making, a consequential decision *before* the decision is made." (Emphasis added.) Under the law, deployers/employers must also provide consumers with a statement disclosing the purpose of the covered AI system, the nature of the consequential decision, and a description of the covered AI system. Additionally, for a consumer adversely affected by an AI system, further notifications must be provided, such as a statement disclosing the principal reason(s) for the consequential decision; "an opportunity to correct any incorrect personal data" used by the covered AI system; and "an opportunity to appeal an adverse consequential decision … which appeal must, if technically feasible, allow for human review." An employer also must post in a "clear and readily available" manner a notice on its website containing various information regarding covered AI systems, such as the types that are currently used, how the employer manages risks of algorithmic discrimination, and "in detail, the nature, source, and extent" of data collected and used by the employer.

d. *Notice to attorney general.* Additionally, employers must disclose to Colorado's attorney general the discovery of algorithmic discrimination—within ninety days after the date of the discovery—that the high-risk AI system has caused.

Colorado Has Provided Affirmative Defenses

Interestingly, the law provides for potential affirmative defenses in any enforcement action by the Colorado attorney general if a deployer/employer discovers and cures a violation as a result of (i) feedback, (ii) "adversarial testing or red teaming" (as those terms are defined by NIST), or (iii) an internal review process *and* the deployer/employer is otherwise in compliance with NIST's Artificial Intelligence Risk Management Framework or another internationally recognized framework for artificial intelligence management.

What's Next?

In addition to closely monitoring for guidance on or amendments to the Colorado AI Act, employers may want to consider the following:

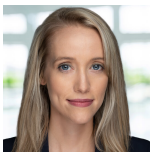
- Inventorying AI uses as part of human resources practices and weighing whether any or all of the uses fall within the current definition of covered high-risk AI systems for the purposes of the act.
- Evaluating whether the organization has or should develop AI policies or frameworks to manage AI systems.
- Commissioning a cross-disciplinary team to monitor AI systems used by the organization, as well as relevant legal developments.
- Assessing whether the organization provides notices about AI systems used. The requirement of notices is a growing trend in AI laws and is also a "promising practice" recommended by the U.S. Equal Employment Opportunity Commission (EEOC).

Currently, many states are actively considering similar AI legislation and regulations. Ogletree Deakins' Technology Practice Group will continue to monitor developments and will provide updates on the Cybersecurity and Privacy, State Developments, and Technology blogs as additional information becomes available.

Follow and Subscribe

LinkedIn | Instagram | Webinars | Podcasts

AUTHORS



Jennifer G. Betts

Office Managing Shareholder, Pittsburgh

Danielle Ochs

Shareholder, San Francisco

Michael H. Bell

Office Managing Shareholder, Denver; Shareholder, Dallas

TOPICS

Colorado , Cybersecurity and Privacy , State Developments , Technology

RELATED ARTICLES

May 15, 2024

Employers May Rescind Previously Protected Leave Under the Oregon Family Leave Act by June 1, 2024

May 13, 2024

Connecticut Expands Paid Sick Law to Establish Entitlements for Most Employees by 2027

RELATED PODCASTS

April 12, 2024

California Pay Data Reporting: Key Updates to Prepare for May 8 Deadline

March 22, 2024

California Workplace Safety: Lessons Learned From Heavy Equipment Accidents