Division of Legislative Services
ISSUE BRIEF

High-Risk AI Systems and Algorithmic Discrimination

By: Falah Al-Falahi, Legislative Research Analyst
April 16, 2026

Overview

Artificial Intelligence's (AI) broad capabilities and its adaptability to learn from and access large datasets of sensitive information have raised ethical concerns about its potential to harm fundamental rights, including discrimination in the system's design and deployment in sensitive areas such as employment decisions and health-care services.

For example, Amazon in 2017 deployed an AI system tasked with recruiting top candidates for open positions. However, a year later, Amazon scrapped its AI recruiting model after discovering that the system was discriminating against female applicants. In another case where AI was potentially deployed, there is a pending class action lawsuit that was filed against United Health Group (UHG) for allegedly using AI models to deny certain medical claims. Moreover, the U.S. Equal Employment Opportunity Commission settled its first-ever AI employment discrimination lawsuit in 2023 after iTutorGroup rejected more than 200 qualified applicants because of their age. These cases have prompted many states to regulate and define these AI systems as "high-risk AI systems" due to their ability to make decisions that pose a significant risk in areas of health, safety, or fundamental rights.

At least 22 states have introduced legislation addressing high-risk AI systems, and 4 states have enacted legislation on high-risk AI systems. Notably, in 2024 Colorado became the first state to enact comprehensive AI legislation which was set to go into effect February 2026. Under the Colorado AI Act, "high-risk" AI models are defined as AI models that are developed and deployed in areas where the AI model is a substantial factor in making a consequential decision[1].Furthermore, Colorado requires developers and deployers of "high-risk" AI systems to meet certain obligations, including exercising "reasonable care" to protect consumers from algorithmic discrimination. Additionally, Colorado's AI Act requires deployers and developers to create risk management programs, produce annual impact assessments, provide notices to workers for consequential employment decisions, and to notify Attorney General within 90 days after discovering algorithmic discrimination.

Since its passage in May 2024, the law has been met with extensive criticism from tech groups and has recently been pushed for implementation to June 2026. Furthermore, with the recent signing of an executive order in 2025 which directs the U.S. Attorney General to establish an AI litigation task force to challenge any state AI laws that are inconsistent with the Executive Order's language, the enforceability of Colorado's AI Act and other state AI laws is currently unknown.

[1] A decision that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of (a)education enrollment, (b)employment, (c)financial lending services,…(e)healthcare services, (f)housing.

Regulatory Safeguards

Colorado along with other states employ various policy tools or levers to regulate the potential for AI systems to discriminate through the following policy mechanisms:

Extending anti-discrimination laws to AI by adapting existing civil rights frameworks.

Audits and Impact assessments are required prior to deployment by deployer. The impact assessment must disclose the intended use cases for the high-risk AI system, an analysis of whether the AI system poses any foreseeable risks of algorithmic discrimination, and categories of data the AI system processes as inputs and outputs. The deployer is also required to review the deployment of the AI system annually to ensure the AI system is not causing algorithmic discrimination.

Consumer protections such as requiring disclosure requirements and granting consumers the ability to appeal decisions conducted by an AI system.

Advantages of Regulating High-Risk AI Systems

Protect consumers rights and safety against discrimination arising from high-risk AI systems.

Promotes trust with AI systems through transparency requirements and an appeal process.

Preventing economic or social harm to consumers that results due to high-risk AI system denying consumers from essential government services or programs.

Challenges of Regulating High-Risk AI Systems

Defining the parameters for liability. Defining at which point does liability shift to the deployer or to the developer, since modification to the AI system can be made by the deployer.

Definition ambiguity. A growing concern among critics of the policy to regulate high-risk AI systems is that the terms will be overly broad. This could result in certain AI systems being unnecessarily defined as high-risk, potentially exposing AI developers to penalties. Additionally, this could create a chilling effect that discourages AI innovation.

Current Events/Compare State's Activity

Maryland and Kentucky direct their respective AI State agency to adopt policies and procedures concerning systems that employ high-risk AI by a unit of State government. (MD SB818) (KY SB4)

New York: introduced a bill in 2025 regulating high-risk AI systems and referenced a national standard for risk management, specifically the National Institute of Standards and Technology (NIST). (SB S1962).

California: California Privacy Protection Agency (CPPA) adopted regulations that granted consumers the ability to opt-out of the use of AI systems in "significant decisions." (regulations)

Utah: requires disclosures when users engage in high-risk AI systems. (SB226)

Illinois: prohibits AI from using protected characteristics or zip codes to discriminate in hiring, promotion, or discipline, and requires high-risk AI audits. (HB 3773)

Considerations for Delaware Legislators

Delaware legislators could promote AI innovation by applying the regulations on high-risk AI systems to only **small AI developers or deployers**.

Delaware legislators could **require human-oversight** for any consequential decisions undertaken by an AI system as mandated by frameworks like the EU AI Act.

Delaware legislators could **distribute liability between developer and deployer** of high-risk AI systems through requiring annual auditing and reporting requirements.

Delaware legislators could **utilize definitions of personal data defined under the Delaware Personal Privacy Act** to define what constitutes data interaction with high-risk AI systems.