

Evolving AI Tools and Reliance in the Workplace: Key Developments Employers Need to Know

WRITTEN BY

Kristalyn Lee | Amanda M. Cummings

It started as merely trying out artificial intelligence (AI) tools. Now, more and more employers (and their employees) are relying on AI for their everyday operations, including drafting emails and summaries, screening and ranking applicants, managing employee performance, and answering routine questions. This expanded role has changed AI from a casual acquaintance into a new “co-worker” that can influence employment decisions, outcomes, and experiences. Employers are reviewing AI tools, assessing risks and deciding which tools are authorized in their workplace and for what purpose. Courts and regulators are also reviewing AI tools more closely, focusing on discrimination, transparency, monitoring, and protection of confidential information.

AI Is No Longer Just a Tool – It’s a ‘Co-Worker’

As AI becomes embedded in workflows, its role can be difficult for employees to distinguish from the input or output of employees. For example, an employer might not know that some resumes never reached an employer’s internal recruiter because an algorithm quietly filtered them out, or that a supervisor disciplined an employee based on AI-generated performance notes that looked polished but incorporated incomplete or biased data. However, when employees blindly rely on the output of AI “co-workers” without careful review or input, the outcome can be low-quality work product, inaccurate analysis, and potential legal liability for their employer.

Anti-Discrimination Laws Are Also Evolving

Troutman Pepper Locke has previously outlined the potential risks when AI meets [DEI and discrimination](#) and [recruiting](#). Another recent decision reinforced those themes. In *EEOC v. iTutorGroup*, the U.S. Equal Employment Opportunity Commission filed an age discrimination lawsuit against an employer, alleging that the automated system it utilized was programmed to reject older applicants based on age cutoffs. These cases and others signal that courts will apply traditional disparate treatment theories when protected characteristics are hard-coded into AI tools, and that employers cannot treat algorithmic filters as a “black box” defense. Accordingly, employers should carefully vet, test, and document the effect of any filters or algorithms (AI or otherwise) before incorporating them into the hiring or screening process and should periodically monitor those tools to identify and remediate any potential bias or disparate impact. In practice, this means understanding how a vendor’s tool functions, conducting pre-deployment and periodic validation or adverse-impact analyses, avoiding the use of protected characteristics (or close proxies) as inputs, and maintaining written records of the evaluation process, plus negotiating contractual provisions that ensure vendor compliance and indemnification. Employers should also involve counsel, HR, and technical personnel in reviewing these tools, and should be prepared to adjust or

discontinue use of any filter or algorithm that produces disproportionate or otherwise potentially legally problematic results.

Other decisions demonstrate that courts can apply familiar discrimination frameworks even when AI sits between the employer and the applicant and/or employee. In *Mobley v. Workday, Inc.*, a California district court case, an employee brought federal and state discrimination claims against the employer's AI vendor, alleging that the vendor's screening tools disproportionately rejected applications based on race, age, and disability. The court allowed those claims to go forward, emphasizing that when an AI system performs hiring functions, the AI can be treated as an "agent" of the employer, much like a human recruiter, and that unintentional algorithmic bias may still create liability even without evidence of discriminatory intent.

A Growing Patchwork of State AI Regulation

As outlined in a recent [article](#) by the Troutman Pepper Locke Labor + Employment Group, states are beginning to regulate AI directly, particularly when it is used to make "high-risk" employment decisions. For example, Colorado's Artificial Intelligence Act, which takes effect on June 30, 2026, requires deployers of certain AI systems to use reasonable care to protect residents from known or reasonably foreseeable risks of algorithmic discrimination and to provide basic explanations and correction rights when AI is involved in significant decisions. Texas has taken a different approach in the recently enacted Texas Responsible Artificial Intelligence Governance Act (TRAIGA), which focuses on intent: the act bars the use of AI with discriminatory intent and provides that disparate impact alone is not enough to establish that intent.

In Illinois, January 1, 2026, marked the effective date of amendments to the Human Rights Act that expressly address the use of AI in employment. These amendments make employers liable for the use of AI systems that have any discriminatory effect, as well as for failing to notify employees when AI will be used in connection with significant employment decisions, such as recruitment, hiring, promotion, renewal of employment, selection for training or apprenticeship, discharge, or discipline. Other states, including California and New Jersey, have signaled that AI-driven decisions fall within existing anti-discrimination frameworks. At the federal level, a recent [executive order](#) on national AI policy signals potential legislation, but in the meantime, employers must still carefully maneuver compliance with a patchwork of state laws and regulations.

Privacy, Monitoring, and Confidential Information

AI-enabled employee monitoring tools also raise legal compliance concerns. Systems that track keystrokes, screen activity, location, or communications may trigger state notice or consent requirements, and aggressive monitoring could possibly "chill" protected concerted activity in violation of the National Labor Relations Act. Illinois now requires explicit consent before using AI to evaluate video interviews or other applicant data, and many jurisdictions require all-party consent to record calls and meetings — creating a potential compliance trap for tools that automatically record or transcribe meetings or other communications. Trade secret protection can also be undermined if employees input sensitive code, customer lists, strategy documents, or any other confidential information into public AI systems. Another potential issue is everyday tools like AI note takers and recorders that capture and store sensitive, confidential information. Once recorded, employers must be vigilant to determine where this confidential information is stored and who has access to such information in order to maintain certain protections, such as attorney-client privilege and access to confidential information. As such, employers should

adopt and enforce clear policies and practices governing AI use in the workplace to mitigate these risks — including explicit limits on entering confidential or trade secret information into public tools, requirements to use only approved AI platforms, and regular training and audits to confirm compliance with monitoring, privacy, and labor?law obligations.

Practical Steps for Employers

To manage the risks associated with the use of AI in the workplace, employers should evaluate the types of AI tools being used and adopt clear AI policies addressing AI usage, including which tools are authorized and for what use, when and how it may be used and when and how and why it is prohibited, with an emphasis on using AI as a tool that requires human review and oversight. Developing these policies and procedures should be a well-rounded, team effort that involves human resources, legal, technical, and compliance issues to understand the intersection between the AI tools used, the implications on the workforce, and parameters that must be set in place to monitor such usage. Employees should be trained on the risks associated with the use of each of the AI tools which are authorized for use and the reasons behind limitations on use as a means to mitigate other risks. A human decision?maker should remain ultimately responsible for all AI use, as privacy, trade secret, confidentiality and discrimination issues could be at risk. Legal, HR, and IT teams should coordinate on vendor selection to understand how the AI tools were developed and tested, and employees should be trained on responsible AI use, including when to scrutinize or override AI recommendations. Treating AI tools as powerful but fallible co-workers — and aligning policies, oversight, and training with that reality — will help employers capture AI's advantages while managing potential risk for such usage, ensuring compliance with developing AI laws and legislation in the employment space, and staying ahead of these evolving expectations.

RELATED INDUSTRIES + PRACTICES

- [Artificial Intelligence](#)
- [Labor + Employment](#)