POLSINELLI | What a law firm should be.™

Considerations for Artificial Intelligence and Employment Law

As artificial intelligence ("AI") technologies become more ubiquitous and advanced, both the advantages and potential risks they pose for employers continue to grow as well. This is especially true with regard to the use of generative AI – that is, AI that can generate original content based on data patterns. This type of AI can produce original images, text, music and designs, among other things. With the rising use of AI, we are seeing a corresponding rise in legislation, guidance and litigation addressing the use and consequences of AI. One area where this is increasingly common is the employment sphere.

AI in the Employment Cycle

More and more, employers are using AI in various aspects of the employment cycle. Recruitment is one of the stages when AI is used most, including through resume screening, video interviews, pre-employment assessment and automated candidate services. During employment, AI may be used in various ways, such as automated employee service, skill development, performance management and in various everyday work tasks.

These usages, though, can pose various risks to employers that use AI.

The Risks of AI in Employment

Title VII and Machine Learning AI

Title VII – the landmark anti-discrimination law – prohibits employers from using neutral tests or selection procedures unrelated to the position and inconsistent with business necessity when those tests or procedures disproportionately exclude persons of a protected class (i.e., race, color, religion, sex, national origin).

When such an effect results from such neutral tests or selection procedures, it is known as disparate impact or adverse impact discrimination. This type of discrimination is generally only an issue with predictive AI tools because that type of AI utilizes algorithms to recognize data patterns and make predictions – which can lead to biased results when the underlying algorithms are biased (even if inadvertently so).

In May 2023, the Equal Employment Opportunity Commission ("EEOC") released guidance specifically addressing the use of AI for employee selection processes. According to the EEOC, AI has an "adverse impact" when the selection rate for one group is "substantially" less than the selection rate for another group. The May 2023 guidance set forth the "Four-Fifths Rule" for determining what "substantially" means. The acceptance rate for a class of applicants is "substantially" different from the acceptance rate of another class of applicants if the ratio of the two rates is less than four-fifths (80%). Not only do employers need to make sure their selection processes are in line with these requirements, but they can still be liable for discriminatory selection procedures even if the AI tool used for the procedures was developed by a third party or administered by an agent.

ADA and Machine Learning AI

Similar to what was done with Title VII, the EEOC issued guidance addressing concerns with the use of AI in interacting with the requirements of the Americans with Disabilities Act ("ADA"). That guidance provides three main examples of AI violating the ADA:

1. If the AI usage results in a failure to provide a reasonable accommodation – this may occur when an applicant or employee requests a reasonable accommodation, and the disability is likely to make it more difficult to use the AI tool or make an assessment less accurate and the employer fails to provide an alternative format.
2. If the AI usage results in an intentional or unintentional screening out of disabled applicants – this may occur when an AI tool results in lower scores for assessments as a result of a disability, such as giving a lower rank to applicants with significant gaps in employment history or with specific speech or movement patterns.
3. If the AI system makes "disability-related inquiries" or conducts "medical examinations" prior to extending a conditional offer of employment – this can also violate the Genetic Information Nondiscrimination Act.

Labor Law and AI

The broad scope of Section 7 of the National Labor Relations Act's right of employees to self-organize and bargain collectively can also be affected by AI usage. The National Labor Relations Board General Counsel issued a memo in October 2022 setting forth numerous ways the use of AI tools can violate Section 7, including when:

- AI tools surveil/gather information regarding employee Section 7 activities – even if merely creating the impression of surveillance;
- Employees are disciplined for protesting the use of AI tools for employee monitoring/management;
- AI tools include personality tests to evaluate an employee's propensity to engage in protected Section 7 activities;
- AI tools use algorithms to make decisions based on union representation;
- AI tools use algorithms that include production quotas or efficiency standards to single out union supporters;
- Employers fail to provide information about the implementation/use of AI technology to employees; and
- Employers fail to bargain with employees over the implementation/use of AI technology in the workplace.

Legislative and Litigation Trends

Cybersecurity

Adding to the growing mix of guidance is November's *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (EO).[1] Among other things, the EO addresses cybersecurity requirements that must be considered by federal agencies and AI developers, given AI's ability to be leveraged by threat actors.

Cybersecurity threats posed by AI – known as *adversarial AI* – include the vivid examples highlighted by Jonathan Care in his article aptly titled "Fight AI with AI."

> [A]n autonomous vehicle that has been manipulated could cause a serious accident, or a facial recognition system that has been attacked could misidentify individuals and lead to false arrests. These attacks can come from a variety of sources, including malicious actors, and could be used to spread disinformation, conduct cyberattacks, or commit other types of crimes.

For these and other safety and security reasons, the EO requires the establishment of an advanced cybersecurity program to develop AI tools to find and fix vulnerabilities in critical software. The EO also includes deadlines by when certain standards must be established for such things as physical and cybersecurity protections (90 days) and safety and security guidelines for use by critical infrastructure owners and operators (180 days).[2]

Data Privacy

Another major concern with AI is its natural intersection with data privacy – AI usage of consumer and employee data lends itself to potential problems with maintaining the privacy of that data. At the same time, many states are taking a stronger approach to data privacy, with numerous states passing data privacy laws in the past year or so, with some of those states – including California, Colorado, Connecticut, Iowa, Utah and Virginia – even specifically addressing AI in their privacy laws.

Beyond just state law, the Federal Trade Commission ("FTC") has also exercised its authority to regulate algorithmic consumer data usage under Section 5 of the FTC Act, Fair Credit Reporting Act and the Equal Credit Opportunity Act. The FTC specifically has encouraged deployers of AI to take steps to:

- Ensure transparency through disclosures;
- Monitor data inputs and outputs to prevent class discrimination;
- Grant user access to delete or correct personal information;
- Ensure output data is accurate;
- Protect the algorithm from unauthorized use or breaches; and

---

[1] **https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/**

[2] *Id.* at §§ 4.2(c) and 4.3(a).

- Implement accountability structure to help maintain compliance.

The FTC further recommends that employers remove any identifying data before entering it into any AI platform.

Data privacy concerns in particular are becoming a heightened concern for employers as courts begin to view employer obligations in protecting such data more broadly. In *Ramirez v. Paradies*, 69 F.4th 1213 (11th Cir. 2023), the Eleventh Circuit found that traditional tort law – and the duty of care, the special relationship between employers and employees, and the foreseeability of harm thereunder – could impute liability to an employer that suffered a ransomware attack on its administrative systems, leading to the unauthorized disclosure of current and former employees' Social Security numbers. With AI potentially increasing the collection of personal information on employees, and courts and legislatures heightening scrutiny on employer protection of that information, employers should take a careful look at their processes and procedures for protecting employee data.

Automated Employment Decisions

New York City has already passed a law regulating automated employment decision tools ("AEDTs"). The law is meant to prevent bias in the use of AEDTs and requires that AEDTs undergo bias auditing within the year prior to use when (a) the employer relies "solely" on the AEDT in making employment decisions; (b) the employer relies on other factors in addition to the AEDT output but weighs the AEDT output more heavily than any other criterion; or (c) the AEDT output is used in a way that can overrule conclusions from other factors, including human decision-making. In addition to the bias auditing, employers must also provide notice to employees and applicants of the AEDTs' use and publish the audit results, and they must retain AEDT records and reveal them to employees upon request. As the use of AI and AEDTs increases, an increase in this type of regulation can be expected.

Additionally, the California Privacy Protection Agency has issued draft regulations for automated decision-making technology ("ADMT"). Under the draft regulations, ADMT has a broad definition and includes any system, software or process (including those derived from AI) that processes personal information and uses computation, either on its own or as part of a system, to make or execute a decision or facilitate human decision-making. There are three main compliance requirements with regard to the use of ADMT: (1) the provision of a notice prior to the use of ADMT that informs employees about the ADMT use and employees' rights with regard to ADMT use, (2) responding to opt-out requests with regard to ADMT use and (3) giving employees the right to access information about ADMT.

Specific AI State Legislation

Many state legislatures, including those of California, Massachusetts, New Jersey and Vermont, as well as the D.C. legislature, have proposed legislation relating to the use of AI in the employment sphere. More states will likely follow suit. These laws would be expected to prohibit "algorithmic discrimination" and put in place notice and accommodation requirements for the use of AI in employment decisions.

EEOC Litigation and Settlement

In May 2022, the EEOC filed an age discrimination lawsuit against a group of affiliated companies employing English-language tutors. According to the EEOC, for a brief period in the spring of 2020, those companies programmed application software to automatically reject female applicants over 55 years old and male applicants over age 60. The lawsuit alleged this screening process affected over 200 applicants who were above the programmed age thresholds. The parties reached an expansive settlement, including a consent decree subjecting the employers to various nonmonetary obligations, including providing notice of the lawsuit to high-level executives and HR employees, retaining a third-party group to conduct extensive training on all federal equal employment opportunity laws, and inviting the rejected applicants to reapply (with reporting obligations to the EEOC). It can be expected this will just be the first of many such actions by the EEOC.

Looking Ahead

The landscape in terms of the use of AI and its regulation is constantly evolving as new technologies develop and become more accessible. With many states already working on legislation to regulate AI usage, the trend can be expected to continue moving forward. The same is true in terms of litigation – both in terms of data privacy and in AI. As has already been seen, the EEOC likely will be focused on the use of AI in employment decisions, and many more lawsuits and settlements can be expected.

Employers navigating in this new arena should keep several things in mind moving forward. Consider auditing vendor AI systems that are being used for potential biased algorithms. Conduct HR and hiring manager training on the proper use of AI systems. Limit employees' access to AI tools to prevent misuse. Implement policies to limit AI use to preapproved circumstances. Provide notice to applications and employees of AI usage. Conduct privacy impact assessments to determine the risk to individuals and applicable mitigation measures. Update incident response plans to address the cybersecurity threats AI may pose to employee data. With an ever-changing world of AI, employers need to be prepared to handle the advancements and challenges that lie ahead.