**DECEMBER 5, 2024 | AI/TECHNOLOGY, PRIVACY & DATA SECURITY**

# AI in the Workplace: Legal Pitfalls and the Department of Labor's Roadmap for Employers

BY DARIUS ROHANI-SHUKLA

**Understanding AI in the Workplace: What Employers Need to Know**

Artificial intelligence (AI) is rapidly transforming how businesses operate. From automating repetitive tasks to streamlining decision-making, AI has become a powerful tool for increasing efficiency and fostering innovation. With its growing adoption, employers face many new questions about how AI should be used in the workplace, what responsibilities businesses have in its implementation, and what legal risks should be considered.

To address these challenges, the U.S. Department of Labor released a guidance document "Artificial Intelligence and Worker Well-Being: Principles and Best Practices for Developers and Employers." This framework provides a structured approach for businesses and developers to think critically about the role of AI in the workplace. While it carries no direct legal force, it has substantial influence as a framework for responsible AI use.

Employers who adopt its recommendations can reduce risks, build trust, and create safer, fairer workplaces. At the same time, the document provides a potential tool for employees or regulators to hold organizations accountable for failures in AI oversight. This blog explores the key aspects of these principles and practices, helping employers understand the framework and its implications for their operations.

**The Role of AI in the Workplace**

AI has the potential to enhance productivity and improve operations in numerous ways. It can automate time-consuming tasks, analyze large datasets to make informed decisions, and even assist in hiring by screening resumes more efficiently.

The Department of Labor's framework is at pains to highlight that AI should be implemented in ways that empower workers, rather than replace them. While the principles outlined below are not mandates, they encourage employers to think about AI adoption as more than a technical upgrade, and demonstrate the DOL's position is that AI is an opportunity to foster trust, improve job quality, and mitigate risks.

**Key Principles for AI in the Workplace**

The framework outlines several principles and best practices for employers and AI developers. Below is a breakdown of these key ideas and what they mean for businesses:

1.  **Centering Workers in AI Development**

One of the foundational principles is ensuring that workers have a voice in how AI is designed and implemented. This means engaging employees in the process of developing AI tools. For example, businesses might host focus groups to gather feedback on new systems to identify potential issues early and build systems that genuinely support employees.

2.  **Governance and Oversight**

AI systems require robust governance structures to ensure they are used responsibly. The framework emphasizes the importance of human oversight, particularly for decisions related to hiring, promotions, scheduling, and discipline.

Employers are encouraged to document how AI is used in these areas and ensure that human managers are trained to interpret AI outputs accurately. This is to prevent over-reliance on automated systems and ensures decisions remain fair and contextually appropriate.

3.  **Transparency in AI Use**

The framework stresses that employees should be informed about how AI systems are being used, what data they collect, and how those systems impact workplace decisions.

For instance, if an AI tool is used to monitor productivity or schedule shifts, employees should understand the criteria it uses and have opportunities to ask questions or challenge decisions.

4.  **Protecting Worker Data**

AI systems often rely on large amounts of data, which raises significant privacy concerns. The framework advises employers to collect only the data necessary for legitimate business purposes and to ensure that it is securely stored and handled responsibly.

The framework also encourages employers to offer workers the right to review and correct any inaccuracies in the data used by AI systems. Employers can comply with this principle by implementing clear data policies and appointing a Data Protection Officer can help businesses meet these expectations.

5.  **Supporting Job Transitions**

AI adoption may lead to changes in job roles or even job eliminations. The framework encourages employers to take proactive steps to retrain or upskill workers whose roles are affected by automation. Some examples of ways of doing this are partnering with workforce development programs or offering in-house training to help employees transition into new roles.

6.  **Avoiding Bias and Discrimination**

One of the biggest challenges with AI systems is the risk of algorithmic bias. If not carefully monitored, AI tools can inadvertently discriminate against workers or job applicants based on protected classes. To mitigate these

risks, employers should conduct regular audits of their AI systems to identify and address any biases. Employers can also confirm with developers that datasets are used to train AI models are representative and inclusive.

**The Legal Implications of AI in the Workplace**

While the framework is not legally binding, it emphasizes that employers must comply with existing labor laws when implementing AI. Key areas of focus include labor rights, anti-discrimination laws, and health and safety standards.

AI-powered systems, particularly those used for monitoring employees, can unintentionally infringe upon labor rights protected under the **National Labor Relations Act (NLRA)**. These rights guarantee employees the ability to organize, form unions, and discuss workplace conditions without fear of retaliation. Misuse of AI tools—such as surveillance systems that track communications or activities—could suppress such discussions or discourage union organizing efforts, exposing employers to legal challenges. Transparent use of AI and clear boundaries are essential to prevent overreach and ensure compliance with these protections.

AI systems also face scrutiny under **anti-discrimination laws** like Title VII of the Civil Rights Act and the Americans with Disabilities Act (ADA). These laws prohibit discrimination based on factors like race, gender, and disability. However, AI decision-making, particularly in hiring and promotions, risks perpetuating bias if trained on skewed historical data. Employers must address these risks by conducting regular audits, using diverse datasets, and ensuring human oversight to rectify any discriminatory patterns in AI decisions.

In the realm of **health and safety**, AI tools designed to optimize workflows or track productivity must not compromise employee well-being. Pushing workers to meet AI-driven productivity targets can lead to overwork, stress, and even physical injuries. Employers are responsible for ensuring that AI usage aligns with OSHA standards and prioritizes safety over efficiency.

Ultimately, employers must develop clear policies around AI usage, promote transparency with their workforce, and supplement AI systems with human oversight to balance innovation with accountability. Addressing these legal and ethical considerations is not merely a suggestion but a critical regulatory obligation. Failure to comply with labor laws, anti-discrimination statutes, and health and safety regulations can result in severe legal consequences, including lawsuits, penalties, and reputational damage. Employers who neglect these responsibilities risk undermining their operations and exposing themselves to significant liability.

**Data Privacy and Security: A Growing Concern**

One of the most critical aspects of the framework is its focus on data privacy. AI systems rely heavily on data, but mishandling this information can erode trust and expose businesses to reputational and legal risks.

The framework provides clear guidance for responsible data use:

- Limit data collection to what is necessary for specific business purposes.
- Implement strong security measures to protect sensitive information.
- Provide workers with transparency about what data is being collected and how it is being used.
- Allow employees to dispute or correct inaccuracies in their data.

**What Employers Should Consider**

As AI becomes more embedded in workplace operations, employers have a lot to think about. Here are a few key questions to guide your approach:

- How will AI affect different groups within your workforce? Are there risks of unintended harm or bias?
- Are you prepared to retrain workers for roles that may evolve due to AI adoption?
- How are you protecting worker data, and do your policies align with best practices for privacy and security?

The Department of Labor's framework provides a valuable starting point for thinking critically about AI in the workplace. While not all businesses will adopt these principles wholesale, they serve as a guide for navigating the complexities of AI implementation. By asking the right questions and implementing thoughtful practices, businesses can ensure that AI adoption is not only efficient but also legally compliant and ethically sound. Ignoring the legal risks—ranging from lawsuits and regulatory penalties to reputational harm—can jeopardize the success of any organization. Employers must prioritize compliance with labor laws, anti-discrimination statutes, and health and safety regulations to avoid these severe consequences. If you have questions or need guidance on navigating the complexities of AI in the workplace, we are here to help.