ROKAS

''AI Act'' at a Glance: Workplace Surveillance and Employee Rights”

The ''AI Act'' is a landmark EU Regulation designed to address the complexities and potential risks related to AI technologies. Its primary objectives include fostering trust and accountability while promoting innovation. Aligned with the core values of the Charter of Fundamental Rights of the European Union, the ''AI Act'' aims to safeguard individuals, businesses, democracy, and the rule of law. Simultaneously, it aims to stimulate innovation and employment, positioning the EU as a pioneer in the adoption of reliable AI technologies.

The ''AI Act'' classifies AI systems into four (4) risk categories: minimal or no risk, limited, high, and unacceptable risk. This classification enables tailored regulatory measures, with particularly stringent requirements for high-risk AI systems, including those used for monitoring and surveillance of employees. High-risk AI systems are those that can significantly impact the health, safety, and fundamental rights of persons within the EU. Annex III of the Regulation enumerates AI systems falling under eight thematic categories automatically classified as high-risk. This includes, among others, the category of employment, employee management and access to self-employment. Specifically, AI systems in employment are categorized into two subcategories: a) systems used for recruitment, advertising and candidate assessment and b) systems used for decisions regarding promotions, terminations, task assignments based on individual behavior or characteristics and monitoring and evaluating individual performance and behavior.

The most common traditional methods of employee surveillance typically include the direct observation by a manager or employer, recording telephone calls, monitoring online activities, and using surveillance cameras. However, new methods of surveillance using AI systems have emerged, offering more advanced and continuous monitoring capabilities. AI-driven tools can, for example, track computer usage, analyze emails, and employ facial recognition for attendance and security purposes. **The greatest risk stems from these tools' ability to aggregate information and derive conclusions that not only affect the working relationship but also intrude upon and potentially distort the employee's personal identity**. These advanced tools provide real-time data and insights but also raise concerns about privacy and the extent of monitoring, requiring careful ethical considerations and regulations like the ''AI Act'' to balance innovation with employees' rights.

The ''AI Act'' prohibits AI applications that pose substantial risks to fundamental rights, particularly in the context of workplace surveillance. It strictly prohibits AI systems that enable indiscriminate or unjustified surveillance or monitoring of employees. This measure aims to restrict employers' use of AI for surveillance purposes, thereby safeguarding employees' privacy and personal dignity. This regulatory framework ensures that AI technologies in the workplace are deployed responsibly and ethically, balancing technological advancements with the protection of individual rights.

In any case, national legislation of individual Member States regarding this issue must be observed, as well as general fundamental principles governing ethical surveillance practices, and in particular:

- **Informed Consent**: Employees should be fully informed about the monitoring tools being used, their purposes, and the data being collected. Obtaining explicit consent ensures awareness and agreement to the surveillance methods.
- **Data Minimization**: Only necessary data for legitimate business purposes should be collected. This principle prevents excessive surveillance, safeguarding employees from unnecessary privacy intrusions.
- **Non-Discrimination**: AI systems must be designed and implemented to avoid discrimination based on race, gender, age, or other protected characteristics. Regular audits and bias mitigation strategies are essential to ensure fairness in monitoring practices.
- **Proportionality and Necessity**: Monitoring should be proportionate to its purpose. For example, tracking productivity may be justified, but constant surveillance without a clear, necessary purpose is unethical and potentially unlawful.

In order to set the safeguards for compliance with the ''AI Act'', the European Commission has proposed guidelines on non-contractual liability related to AI, through the "AI Liability Directive". These guidelines aim to ensure that victims of AI-related damage can effectively seek compensation. The key aspects include:

- **Reversal of Burden of Proof**: In cases where proving that the AI system caused harm is challenging, the burden of proof may be shifted to the defendant, such as the employer. This approach ensures that victims are not unfairly disadvantaged by the complexity of AI technologies.
- **Strict Liability for High-Risk AI**: Providers and users of high-risk AI systems may be held strictly liable for damages caused by these systems. This reinforces the need for robust risk management and compliance practices.

In conclusion, the ''AI Act'' endeavors to establish a framework that facilitates the beneficial use of AI in workplaces, while also protecting employees' rights and fostering principles of fairness, transparency, and accountability. Implementing AI technologies in the workplace requires a balanced approach that not only harnesses AI's potential for innovation but also upholds the rights of employees and nurtures trust. It is advisable for employers to proactively develop policies that define the ethical and transparent deployment of AI, providing clear guidelines on when and how AI tools can be utilized within the employment context. Through these measures, employers can seamlessly integrate AI advancements while demonstrating a steadfast commitment to fairness and responsibility, thereby positioning themselves at the forefront of technological progress.

ROKAS

Key Contacts

Elianna Maratou
Associate
E: e.maratou@rokas.com
www.rokas.com

Maria Katsioti
Associate
E: m.katsioti@rokas.com
www.rokas.com