The Time to (AI) Act is Now: A Practical Guide to Emotion Recognition Systems under the AI Act

July 19, 2024

The European Union's AI Act represents a significant step forward in the regulation of artificial intelligence technologies, particularly concerning the use of emotion recognition systems.

These systems, which infer or identify emotions from biometric data, pose unique challenges and risks that necessitate strict regulatory measures.

A. Overview of Prohibited AI Practices

Defining Emotion Recognition Systems

According to Article 3(39) of the EU AI Act, an "emotion recognition system" is defined as an AI system that identifies or infers emotions or intentions based on biometric data. Biometric data, as per Article 3(34), includes any personal data resulting from technical processing of physical, physiological, or behavioural characteristics such as facial images or fingerprints. Recital 18 further elaborates that emotion recognition systems encompass AI technologies that identify a range of emotions including happiness, sadness, anger, and more. However, it excludes systems detecting physical states like fatigue unless these are used for safety purposes, such as preventing accidents involving pilots or drivers.

Prohibitions and High-Risk Classifications

The EU AI Act takes a cautious approach towards the deployment of emotion recognition systems in sensitive environments. Article 5(1)(f) outright prohibits the use of these systems in workplaces and educational institutions, unless they serve a medical or safety purpose. This prohibition stems from concerns articulated in Recital 44, which highlights the significant scientific uncertainties and potential discriminatory outcomes associated with these technologies. The variability in emotional expressions across different cultures and individuals can lead to unreliable and biased results, thus justifying their restricted use in contexts where power imbalances are pronounced.

Moreover, Annex III of the AI Act categorises emotion recognition systems as high-risk AI systems, subject to stringent regulatory requirements. This classification is rooted in Recital 54, which underscores the potential for biased and discriminatory outcomes, particularly when these systems are used for critical applications involving biometric data.

Transparency and Data Protection Obligations

Transparency is a cornerstone of the EU AI Act's regulatory framework. Article 50(3) mandates that deployers of emotion recognition systems must inform individuals exposed to these technologies about their operation. This requirement ensures that individuals are aware of when their biometric data is being processed to infer emotions. This transparency obligation is complemented by the GDPR, which governs the processing of personal data, including biometric data, under Regulations (EU) 2016/679 and (EU) 2018/1725.

The GDPR, particularly through its stipulations on special categories of personal data under Article 9(1), reinforces the stringent protections around biometric data. Any processing of such data must comply with the GDPR's requirements, ensuring that the rights and freedoms of individuals are safeguarded. Recital 132 of the AI Act reiterates that transparency obligations must be fulfilled in a manner accessible to all, especially considering the needs of vulnerable groups such as individuals with disabilities.

Balancing Innovation and Regulation

The EU AI Act's stringent measures on emotion recognition systems reflect a balanced approach aimed at fostering innovation while protecting fundamental rights. By categorising these systems as high-risk and imposing strict transparency and data protection obligations, the Act seeks to mitigate the potential harms associated with these technologies.

Recital 63 clarifies that the high-risk classification does not inherently legalise the use of emotion recognition systems under other Union or national laws. Instead, their deployment must always align with existing legal frameworks, including the Charter of

Fundamental Rights of the European Union and the GDPR. This ensures a comprehensive legal oversight that transcends the AI Act's provisions, embedding robust safeguards against the misuse of biometric data.

B. Key Dates:

- 12 July 2024: The AI Act published in the Official Journal.
- 1 August 2024: The AI Act will become law.
- 2 February 2025: Article 5 Emotion Recognition Systems in the workplace or educational settings are banned.
- 2 August 2026: Rules on Annex III Emotion Recognition Systems come into effect.

C. Enforcement and Penalties

- Non-compliance with the rules on Prohibited AI Systems will attract substantial administrative fines of up to €35,000,000 or, if an undertaking, 7% of the offender's total worldwide annual turnover, whichever is higher. Non-compliant AI systems can also be taken off the EU market.
- The AI Act imposes significant fines for non-compliance with its provisions, especially for high-risk AI systems. Non-compliance with specific obligations related to operators or notified bodies can result in administrative fines of up to €15 million or, if the offender is an undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher. This includes obligations of providers (Article 16), authorised representatives (Article 22), importers (Article 23), distributors (Article 24), deployers (Article 26), and requirements and obligations of notified bodies (Article 31, Article 33(1), (3) and (4), or Article 34), as well as transparency obligations for providers and deployers (Article 50).
- Supplying incorrect, incomplete, or misleading information to notified bodies or national competent authorities in response to a request can result in fines of up to €7,500,000 or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.
- For small and medium-sized enterprises (SMEs), including start-ups, each fine is capped at the lower of the specified percentages or amounts.

D. Steps to Compliance:

1. Understand the Scope and Definitions

- Emotion Recognition Systems: Ensure your system fits the definition in Article 3(39), identifying or inferring emotions from biometric data as outlined in Article 3(34).

2. Assess Prohibitions and High-Risk Classifications

- Prohibitions: Verify that your use case does not fall under prohibited scenarios, such as in workplaces or educational institutions, unless for medical or safety purposes (Article 5(1)(f)).
- High-Risk Systems: Determine if your system is classified as high-risk under Annex III, which requires stringent regulatory compliance.

3. Implement Transparency Measures

- Inform Affected Individuals: As mandated by Article 50(3), inform individuals when their biometric data is being processed to infer emotions. Ensure this information is accessible, considering the needs of vulnerable groups (Recital 132).

4. Ensure Data Protection Compliance

- GDPR Alignment: Align your data processing activities with the GDPR requirements, particularly regarding special categories of personal data (Article 9(1) GDPR).
- Safeguards: Implement appropriate safeguards to protect the rights and freedoms of individuals, as required by the GDPR and reiterated in Recital 132 of the AI Act.

5. Conduct Risk Management

- Risk Assessment: Perform a thorough risk assessment to identify potential biases and discriminatory outcomes, as highlighted in Recitals 44 and 54.
- Mitigation Measures: Implement measures to mitigate identified risks, ensuring the system's fairness and reliability.

6. Maintain Documentation and Records

- Record Keeping: Maintain detailed records of compliance efforts, including transparency measures, risk assessments, and data protection safeguards.

7. Engage with Regulatory Authorities

- Consultation: Engage with relevant regulatory authorities to ensure your compliance strategy aligns with the latest regulatory expectations and guidelines.

8. Continuous Monitoring and Improvement

- Ongoing Review: Continuously monitor the performance of your emotion recognition system and review compliance measures regularly.
- Updates and Training: Keep your team informed about updates in regulations and provide regular training on compliance requirements.

9. Legal and Ethical Considerations

- Legal Alignment: Ensure your system's deployment aligns with the Charter of Fundamental Rights of the European Union and other relevant legal frameworks.
- Ethical Standards: Adhere to ethical standards, promoting transparency, fairness, and accountability in the use of emotion recognition technologies.

The regulation of emotion recognition AI systems under the EU AI Act marks a significant advancement in AI governance. By defining these systems, identifying their risks, and embedding stringent transparency and data protection measures, the EU aims to harness the benefits of AI while mitigating its risks. The interplay with the GDPR further strengthens the regulatory landscape, ensuring that the deployment of emotion recognition technologies respects individual rights and maintains public trust. As AI continues to evolve, such comprehensive regulatory frameworks will be crucial in balancing innovation with ethical considerations.

For further guidance and support on AI compliance, please contact Barry Scannell, Leo Moore, Rachel Hayes, or any member of the William Fry Technology Department.

Contributed by Thomas Martin.