Biometric Identification and Categorization

Rules for facial recognition systems.

Co-authored with Victoria Hordern, **Taylor Wessing**, *Partner*

15 September 2025

---

5. Specific Provisions for Certain AI Systems — Sectors, Risks, Safeguards, Limits

5.1 Biometric Identification and Categorization	5.2 AI in Employment and Recruitment	5.3 AI Applications in Education and Training	5.4 AI in Law Enforcement and Border Control
Rules for facial recognition systems.	*Preventing bias in hiring algorithms.*	*Protecting fairness in learning systems.*	*Managing surveillance and policing AI.*

The European Union's Artificial Intelligence Act (AI Act) establishes a comprehensive legal framework for the deployment and use of artificial intelligence technologies, with particular emphasis on systems involving biometric identification and categorization, such as facial recognition. These provisions are designed to mitigate risks to fundamental rights and ensure that AI applications operate within ethical and legal boundaries.

Not all uses of biometric data by an AI system is regulated under the AI Act. For instance, an AI system intended to be used for biometric verification where the sole purpose is to confirm that a specific individual is who they claim to be is not regulated under the AI Act, but would be subject to other laws.

Defining Biometric Identification and Categorization

Biometric identification refers to the automated recognition of individuals based on their unique physical, physiological, behavioral or psychological characteristics, including facial features, fingerprints, and iris patterns. This process typically involves comparing captured biometric data against stored data

within a reference database to establish or confirm a single individual's identity. Biometric categorization, on the other hand, involves assigning individuals to specific groups based on their biometric data, such as categorizing people by age, gender, or ethnicity. While these technologies offer significant utility in various sectors, they also pose substantial risks related to privacy, discrimination, and civil liberties.

Prohibited Practices Under the AI Act

The AI Act identifies certain AI applications as posing an unacceptable risk and, consequently, prohibits their use. Among these are specific practices related to biometric identification and categorization:

- Untargeted Scraping of Facial Images: The Act bans the creation or expansion of facial recognition databases through the indiscriminate scraping of facial images from the internet or closed-circuit television (CCTV) footage. This measure aims to prevent the unauthorized collection and processing of individuals' biometric data without their consent or knowledge, addressing significant privacy concerns.
- Biometric Categorization Based on Sensitive Characteristics: The use of AI systems for biometric categorization that sorts individuals based on sensitive attributes, such as race, religion, or sexual orientation, is prohibited. This provision seeks to prevent discriminatory practices and the potential reinforcement of societal biases through AI technologies but does not apply to labelling or filtering of lawfully acquired biometric datasets or categorising biometric data in the area of law enforcement.
- Law enforcement use of biometrics: The starting point is that the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes is prohibited. However, see below for exceptions to that prohibition.

Permitted use of biometric data for law enforcement purposes

Certain AI systems using biometrics systems in publicly accessible spaces for law enforcement purposes are permitted under strict conditions. The AI Act imposes stringent requirements on these systems to ensure their responsible deployment:

- Real-Time Remote Biometric Identification: The use of real-time remote biometric identification systems, such as live facial recognition in publicly accessible spaces, is generally prohibited. However, exceptions are made for specific law enforcement purposes, including the search for missing persons or the prevention of imminent terrorist threats. These exceptions are tightly regulated, must meet necessary and proportionate safeguards (including a fundamental rights impact assessment) and require prior judicial or administrative authorization to prevent misuse.
- Post Remote Biometric Identification: AI systems that perform biometric identification after a significant delay (i.e. the data has already been captured and the comparison and identification only occurs after a delay), known as post remote biometric identification, are permitted under the Act for the investigation of a criminal offence. Such use is contingent upon obtaining authorisation from a judicial or administrative authority, and ensuring that the deployment of these systems is limited to what is strictly necessary for the investigation.

Regulation of High-Risk AI Systems

Other uses of biometrics by AI systems are classified as high-risk under the AI Act. These are:

- Remote biometric identification systems
- AI systems intended to be used for biometric categorisation, according to sensitive or protected characteristics based on the inference of those characteristics
- AI systems intended to be used for emotion recognition

Safeguards and Compliance Obligations

For high-risk AI systems, including certain facial recognition technologies, the AI Act mandates several safeguards to ensure ethical and lawful operation including:

- Data Quality and Governance: Providers must ensure that biometric data used by AI systems is accurate, representative, and collected in compliance with data protection laws. Robust data governance practices are essential to prevent biases and protect individual privacy.
- Transparency and Accountability: Operators of high-risk AI systems are required to maintain detailed documentation, including records of the system's purpose, functionality, and decision-making processes. This transparency facilitates accountability and enables oversight by regulatory authorities.
- Human Oversight: The Act emphasizes the necessity of human oversight in the operation of high-risk AI systems. Human operators must have the authority to intervene and, if necessary, deactivate the system to prevent harm or legal violations.
- Security Measures: Providers must implement robust cybersecurity measures to protect AI systems from unauthorized access and data security breaches, safeguarding the integrity and confidentiality of biometric data.

Implications for Stakeholders

The provisions of the AI Act have significant implications for various stakeholders involved in the development and deployment of biometric identification and categorization systems. The strictest rules apply for AI systems using biometrics for law enforcement purposes. But certain other key requirements apply in general:

- Developers and Providers: Entities developing AI systems for biometric identification must design their technologies in compliance with the Act's requirements, incorporating necessary safeguards from the outset. This includes conducting thorough risk assessments and ensuring adherence to data protection standards.
- Deployers and Users: Organizations using these AI systems must be vigilant in their application, ensuring that their use aligns with legal provisions and does not infringe upon individuals' rights. This involves obtaining appropriate authorizations and implementing measures for ongoing monitoring and compliance.
- Regulatory Authorities: Regulators are tasked with overseeing the implementation of the AI Act, conducting audits, and enforcing compliance. They play a crucial role in interpreting the Act's provisions and providing guidance to stakeholders..

Conclusion

The AI Act represents a significant step in regulating the use of artificial intelligence, particularly concerning biometric identification and categorization systems like facial recognition. By prohibiting certain high-risk practices and imposing strict requirements on others, the Act seeks to balance technological innovation with the protection of fundamental rights. Stakeholders must navigate these regulations carefully, ensuring that their AI applications are both effective and compliant with the established legal and ethical standards.

Glossary

Act or EU AI Act: European Union Artificial Intelligence Act

AI: Artificial Intelligence

Board: European Union Artificial Intelligence Board

EU: European Union

SME: Small and Medium-Sized Enterprise

How can we help?

AI & Partners
Amsterdam - London - Singapore

AI & Partners ' –AI That You Can Trust'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.