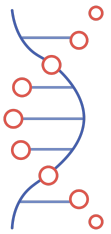
UNDERSTANDING ARTIFICIAL INTELLIGENCE

Biometrics & AI – Explained



This explainer on biometrics and AI is part of CCIA Europe's 'Understanding AI' series, which aims to inform EU policymakers and the wider public about important concepts related to artificial intelligence (AI) and the EU regulatory framework.

What are biometrics and how are they linked to AI?

Biometrics refer to **unique physical and behavioural characteristics of individuals**, such as **fingerprints, facial features, voice, or typing patterns**. Biometrics are particularly relevant in AI applications used for security and safety purposes, because they offer a reliable and convenient way of identifying and verifying individuals. AI technologies have significant capacity to rapidly process and analyse biometric data.

How are biometrics used in practice?

Biometrics can be used in multiple AI applications and in different contexts. **Facial or fingerprint recognition technology that grants secure access to a person's phone** is a well-known example of the use of biometric technology.

Biometric AI systems are often used to **control access to secure areas**, for example in airports or banks. They also help with **identity verification during online transactions** to prevent identity theft and enhance security. Law enforcement agencies also use biometrics to identify suspects or missing persons through fingerprint or facial recognition.

However, the use of biometric AI systems is **not limited to safety and security applications**. Biometrics are also used in everyday applications such as **virtual assistants controlled by voice** like Apple's Siri, Amazon's Alexa, or Google's Assistant.

What are the implications for AI policy?

As biometrics can be used to uniquely identify individuals, privacy must be front and centre in any policy. This is not new, and biometric data is already subject to stringent legal requirements.

In Europe, the General Data Protection Regulation (GDPR) **provides a comprehensive EU framework for the processing of biometric data**, which is subject to specific safeguards as it falls within the scope of "specific categories of personal data".

Beyond the existing requirements and safeguards applicable to the use of biometric data, the EU's **AI Act proposal introduces a number of new requirements** for the use of biometrics in certain AI systems, and even prohibits certain AI applications in this area.

Initially, the European Commission proposed to ban the use of so-called 'real-time remote biometric identification systems' in publicly accessible spaces for law-enforcement purposes. Examples of these are systems able to identify a person in the street using CCTV camera footage. The objective of the ban proposed by the Commission was to prohibit potential forms of mass surveillance in the EU, which is commendable.

However, the European Parliament has considerably expanded the list of provisions and introduced new provisions related to biometric AI systems. Useful, **low-risk applications like using voice biometrics to control smart home devices now risk being banned** from the EU under these rules.

Indeed, recent proposals to **completely ban the use of real-time remote biometric identification systems in publicly accessible spaces and ban the use of biometric categorisation systems** are unnecessarily broad.

Facial recognition, for example, has proven useful for multiple applications including **establishing the age of children online and fighting the dissemination of child sexual abuse material (CSAM)**. It can also be used to detect deep fakes or to mitigate bias in datasets.

Parliament also proposes to **ban emotion-recognition systems in the workplace**, despite their potential use in **protecting the health and safety of people**. For instance, AI-powered systems can use facial recognition to identify whether the driver of a truck is fatigued or drowsy, instantly activating an alarm to ensure they do not fall asleep. Such **lifesaving AI applications would be entirely prohibited**.

What are sensible rules for AI use of biometrics?

The use of biometrics is **already subject to comprehensive rules and safeguards** in the EU. Sensible rules for biometrics in the **AI Act must be clearly targeted at harmful applications** in order to avoid unintended consequences such as mass surveillance.

But to realise the numerous potential positive applications of biometrics in AI, the rules must be carefully balanced. Only truly harmful applications should be prohibited.