How does facial recognition work?

KS3 KS4 Ages 11-16 ⏰ 3 min read

Facial recognition is software that identifies or verifies a person by analysing their face. It converts the geometry of a face into a mathematical representation — a "faceprint" — and compares it against a database to find a match.

How does it work technically?

A camera captures an image. Software detects a face within it and maps key landmarks — the distance between the eyes, the width of the nose, the shape of the jawline, the depth of the eye sockets. These measurements are converted into a numerical vector — essentially a long string of numbers that acts as a unique identifier for that face. This vector is compared against stored vectors in a database. If it's close enough to a stored entry (above a confidence threshold), it's called a match.

Your face is like a fingerprint, but with more data points and readable from a distance. Facial recognition converts that "fingerprint" into numbers: "eyes 62mm apart, nose bridge 18mm wide, jawline angle 112 degrees" — converted into a mathematical point in a very high-dimensional space. Finding a match means finding the stored face whose mathematical point is closest to the one just measured. The closer the points, the more confident the match. Modern neural network-based systems find these mathematical representations automatically from training on millions of faces, rather than using manually specified measurements.

Where is it used?

Phone unlock features (Apple Face ID, Android face unlock) verify that the face matches the one registered to the device. Airport border control increasingly uses it to match faces to passport photos. Retailers use it to identify known shoplifters. Police forces in the UK and elsewhere use it in CCTV footage analysis and live monitoring of crowds. China has deployed it at extraordinary scale as part of broader surveillance infrastructure.

Why is it controversial?

Several reasons. **Accuracy gaps**: multiple studies have found that many facial recognition systems are significantly less accurate on darker-skinned faces and on women, partly because training datasets contained disproportionately white male faces. A false positive — incorrectly identifying someone as a suspect — can have serious consequences. **Privacy**: mass surveillance without consent raises profound civil liberty concerns. **Chilling effects**: if people know they're being identified everywhere they go, behaviour changes — people may avoid protests or political gatherings. These concerns are prompting regulation in the UK and EU, though the legal framework is still developing.