# ICO launches AI and biometrics strategy to tackle risks and rebuild public trust



The UK Information Commissioner’s Office (ICO) has unveiled a wide-ranging AI and Biometrics Strategy aimed at managing the risks of emerging technologies while safeguarding individual rights. The plan responds to growing public concerns over artificial intelligence, particularly in police facial recognition and automated decision-making in recruitment and public services.

Launched recently, the strategy outlines a proactive regulatory agenda focused on high-risk applications that deliver public benefits but carry significant ethical concerns. Key measures include a statutory code of practice for AI, audits of police use of facial recognition, and guidance on the use of personal data in training generative AI models.

“The same data protection principles apply now as they always have—trust matters, and it can only be built by organisations using people's personal information responsibly,” said Information Commissioner John Edwards. His remarks underscore the ICO’s ambition to rebuild public confidence in AI technologies.

Despite mounting interest, adoption of AI tools remains limited. In 2024, just 8% of organisations used AI for decision-making involving personal data, and only 7% employed facial or biometric recognition. This slow uptake reflects public scepticism, particularly around biometric surveillance and algorithmic hiring practices.

To enhance accountability, the ICO plans to audit how police use facial recognition systems and will publish its findings. This follows rising concerns over bias, transparency and fairness in AI systems. A recent report from the Ada Lovelace Institute called for comprehensive legal clarity, highlighting serious gaps in current UK regulation of facial recognition in both public and private sectors.

Critics have described the UK’s regulatory environment as a “wild west” for biometrics, warning of unchecked misuse and threats to civil liberties. In 2024 alone, police scanned nearly five million faces, leading to more than 600 arrests. While the Home Office defends the technology as essential for policing, campaigners argue that stronger legal safeguards are urgently needed.

The ICO has reaffirmed its commitment to enforcement, stressing the importance of proportionality, accuracy and bias mitigation in deploying biometric tools. Its strategy promotes transparency and fairness as foundational principles for any future AI implementation.

As the regulatory landscape evolves, the ICO’s initiative marks a pivotal step in shaping how AI and biometric technologies are governed in the UK. The strategy calls for ongoing dialogue between developers, regulators and civil society to ensure that these powerful tools serve the public interest and respect fundamental rights.

Created by [Amplify](https://www.hbmadvisory.com/amplify): AI-augmented, human-curated content.

## Bibliography

1. <https://www.computing.co.uk/news/2025/ai/ico-unveils-ai-and-biometric-regulation-plan> - Please view link - unable to able to access data
2. <https://www.ft.com/content/09ce1755-554e-43c9-90ad-8e07196763b0> - A report by the Ada Lovelace Institute has raised urgent concerns about the UK's regulation of facial recognition technology, calling for comprehensive legislation and a dedicated regulator. The Institute highlights significant gaps and inconsistencies in the current governance of biometrics, warning that the legal framework is insufficient to address the growing use of facial recognition by police and private companies. In 2024, UK police scanned nearly 5 million faces, resulting in over 600 arrests, and the technology is increasingly used in retail and sports venues. Critics argue that the lack of clear legal boundaries makes the UK a 'wild west' and jeopardizes human rights, particularly with the emergence of AI systems capable of analyzing emotions and intentions. Although the government acknowledges the need for potential new laws, current oversight falls behind other regions like the EU and some U.S. states that have introduced strict limits. Privacy advocates stress the urgent need for safeguards to prevent misidentification and protect civil liberties. While the Home Office defends facial recognition as a valuable policing tool, campaigners emphasize the imperative for modern, targeted legislation to ensure lawful and ethical use.
3. <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/04/statement-on-police-use-of-facial-recognition-technology-frt/> - An ICO spokesperson stated that facial recognition technology (FRT) can aid in crime prevention and detection but must be necessary, proportionate, and meet fairness and accuracy expectations. The ICO's role is to scrutinize its use to ensure compliance with data protection law. They continue to work with users and the public to support understanding of how the law applies. The ICO has renewed its focus on police use of FRT and will publish further details when launching its AI and biometrics strategy later in the Spring.
4. <https://www.biometricupdate.com/202503/uk-ico-warns-biometric-tools-may-pose-privacy-compliance-risks> - The UK Information Commissioner’s Office (ICO) has issued a two-pronged warning about using biometric technologies. They want the public to know that new products and services using biometric data might not have sufficient privacy safeguards. And businesses need to be aware of proportionality, accuracy, and bias issues before deploying biometric technologies. A report from MLex quotes Stephen Almond, who leads the technology and innovation department at the ICO, speaking at a recent UK data protection conference: 'I really recommend for those of you who are looking at uses of biometric technologies, which are often presented as this great time-saving mechanism at work, to actually pause and just think.' While the sales pitch for biometrics might sound great, customers need to ensure the tools they’re deploying meet standards and adhere to guiding principles – for example, 'are we really meeting those expectations around proportionality?' and 'are we giving people the sorts of choices and presenting this in a way where we could demonstrate that there is freely given consent?' To help businesses navigate questions like these, the ICO plans to launch a new strategy on AI and biometrics in the spring. It is also working on a statutory code of practice on AI and automated decision making, which Almond says 'is clearly going to span all of this territory as well.'
5. <https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/> - Artificial intelligence (AI), including biometric technologies, is a priority area for the ICO due to its potential to pose a high risk to individuals and their rights and freedoms. Personal information fuels much of these technologies’ innovation so it must be used responsibly to build public trust and drive growth and improved efficiency. While not an exhaustive list, our current areas of focus include: generative AI; foundation models; Code of Practice on AI and Automated Decision Making; Automated Decision-Making (ADM) systems; AI and children; AI and online safety; police use of biometrics technologies; and recommender systems.
6. <https://datamatters.sidley.com/2024/05/22/ico-publishes-its-strategic-approach-to-regulating-ai/> - The ICO's strategic approach to regulating AI focuses on several key areas, including: (i) foundation models; (ii) high-risk AI applications; (iii) facial recognition technology and biometrics; and (iv) children and AI. The strategy explains how the principles set out in the government’s AI Regulation White Paper consultation mirror to a large extent the statutory principles which the ICO already oversees as the UK’s data protection authority. The ICO outlines in more detail how its principles are aligned with the AI Regulation White Paper principles (such as 'safety, security, robustness,' and 'fairness'), while noting that the government’s approach is not designed to 'duplicate, replace or contradict regulators' existing statutory definitions of similar principles.'
7. <https://www.pinsentmasons.com/en-gb/out-law/news/ico-uk-strategic-approach-ai> - The UK Information Commissioner’s Office (ICO) has set out its strategic approach to artificial intelligence (AI) regulation, listing AI’s application in biometric technologies, protection of children’s privacy, and online tracking as its three focus areas for 2024-25. Although there have been some recent indications that the UK government is actively considering AI legislation, the official position remains as set out in a March 2023 AI White Paper. The paper noted that 'rigid and onerous' legislative requirements on businesses could hold back AI innovation. Instead, the existing regulators, such as the ICO, will issue principles on a non-statutory basis using domain-specific expertise to the context in which AI is used.