pixinoo via iStock

LEGISLATION

What the EU's planned law on AI means for biometrics

Artificial intelligence is advancing quickly – and Brussels is intent on curbing AI errors and overreach. Here's what businesses in the UK need to know about its proposals

Natasha Khullar Relph

The World Cup is currently under way in Qatar, and alongside the thousands of fans in the eight stadiums and on the streets of Doha are 15,000 CCTV cameras – all hooked up to facial recognition systems.

Touted by the organisers as a new standard for global sporting event security, this network of facial recognition-equipped security cameras is meant to catch any potential threats and feed them into a command-and-control centre known as Aspire. Qatar, though, is not alone in deploying this technology. Over the years, security and surveillance systems have become commonplace in soccer clubs and stadiums across the world, including in Europe. As they have proliferated across the continent, so have the cases of misidentification and discrimination.

At the 2017 Champions League final in Cardiff, more than 2,000 people were wrongly identified as possible criminals. In 2019, a 20-year-old fan was banned from the Dutch club FC Den Bosch after being falsely accused of violently confronting supporters and entering restricted areas, based on data from smart cameras. An experiment by the ACLU of Massachusetts using Rekognition, a widely available facial recognition software, led to 27 professional athletes being falsely matched to individuals in a mugshot database.

As facial recognition technology, valued at $3.97bn (£3.36bn) in 2018, has become increasingly common in the everyday life of citizens – from school lunch queues to banking services – questions about privacy and misuse are increasingly being raised. Without a robust legal framework in place that can guide the use of facial recognition and other AI technologies, many worry that great harm can be perpetuated by companies and governments acting in bad faith.

"When you deploy technology to surveil a crowd, you're already violating so many principles of due process," says Iverna McGowan, the director of the Center for Democracy and Technology's (CDT) Europe office. "Normally, you would need at least a warrant or a court order to place an individual under that type of surveillance. But if you're deploying facial recognition in a crowd setting, then you are automatically violating constitutional rights in all our countries."

The European Union is working to improve matters. The proposed AI Act aims to regulate the AI sector and set a global standard for AI oversight by guaranteeing the safety and fundamental rights of individuals and businesses. The legislation, which is currently being amended by members of the European Parliament and EU countries, would have reach beyond the EU's borders in much the same way as the EU's General Data Protection Regulation (GDPR), which applies to any business or institution that serves EU customers. And as with GDPR, the penalties for violations would be substantial: up to €30m (£26m) or 6% of global revenues, whichever is higher.

The proposal divides AI use into risk categories with a regulatory structure that seeks to ban some uses of AI, such as 'dark patterns' or 'subliminal techniques' that manipulate people, while only lightly regulating 'low-risk' categories. High-risk use cases, such as the use of AI in critical infrastructure, law enforcement, migration, border patrol, employment and education, will be heavily regulated with strict rules on transparency and data quality.

Instances of unintentional AI bias, particularly in the finance, real estate and education sectors, have been particularly commonplace. There have been reports of certain groups, including women, migrants and people of colour, denied housing or having their access to credit restricted. Since AI models are based on historical data that has been provided, any bias in the data tends to show up in future decision-making. This was demonstrated in 2020 when British students, unable to take their A-level exams due to the pandemic, were awarded scores based on an algorithm. It was later revealed that the AI had been biased towards students from wealthier schools and the results had to be scrapped.

Wilson Chan is the co-founder and CEO of Permutable, a technology start-up that creates AI solutions. "If you look at the cases that the proposed legislation talks about, the focus is on the vulnerable consumer, such as where it affects decisions with children," he says. "Those use cases represent a small fraction of how AI is being used."

For B2B companies like Permutable, which work with corporates looking to embrace AI for the first time or to adopt it into their product line, Chan says the issue is more that they're effectively approaching clients with a black box technology. "The first thing they try to do is some kind of audit around it and it's an issue for compliance departments, who ask, 'What are you actually doing, what is the product actually doing?'"

That's going to be one of the things to be addressed with the AI Act, says Chan, in that companies will have to be more conscientious about the AI used, especially if the end product is affecting someone in a vulnerable position.

One of the biggest battlegrounds around the act is biometric technology, including facial recognition. While GDPR offers some protections in this regard, it does contain exceptions, such as when the information is essential for employment, social security and social protection law. Countries like Germany have pushed for tighter restrictions on facial recognition technologies, even calling for an outright ban, but many European capitals worry that outlawing the technology could impact public security and police forces' ability to keep people safe.

Most experts agree that there are positive use cases for the technology and facial recognition can make certain identification aspects easier. But the more draconian surveillance measures, such as the mass collection of the identities of people at protests or undocumented migrants, make it a no-go zone. "This is a contentious use of technology that is extremely prone to error. Targeted facial recognition and biometric surveillance, really, in public places, is a threat to human rights and dignity that has to be prohibited," says McGowan. "Obviously, there are some stakeholders on the other side of this debate – whether that's in law enforcement or companies that profit from deploying these types of technologies – that would prefer these types of technology not to be prohibited. That's where some of the most heated debates are at the moment."

While the legislation is finalised – and the details won't become available until next year at the earliest – one thing is clear: the impact will not be the same on every business.

For companies where the use of AI falls under the low-risk category, compliance will be far simpler and less costly than for those that collect private user data or rely on AI-based ID tools. This could be harder than it seems. A survey by Boston Consulting Group shows that while 85% of organisations with AI solutions have defined responsible AI to shape product development, only 20% of organisations have fully implemented these principles.

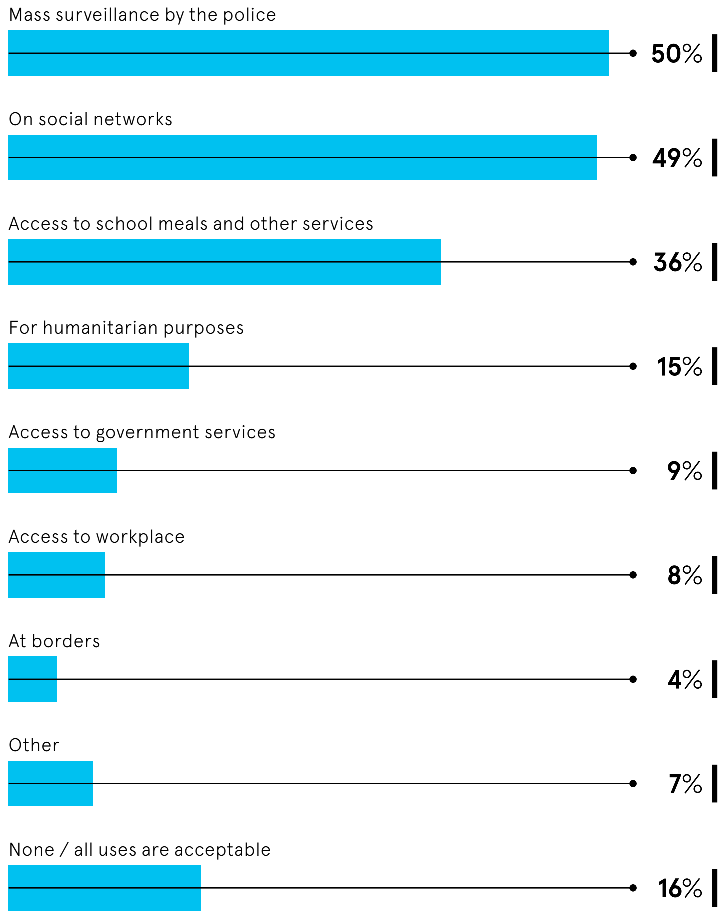
Businesses with high-risk AI systems will, in coming years, face a legal requirement to meet a defined list of criteria before operating in the EU single market. Transparency and ethical compliance frameworks will be the key to success.

"It will hopefully make companies like ours act smarter with the data and use less of it," says Chan. "Can we lift the hood on the black box and show clients what it's doing and how it's working? That's what we're trying to address." ●

> Countries like Germany have pushed for tighter restrictions on facial recognition technologies, even calling for an outright ban

THE PUBLIC IS LUKEWARM ON THE USE OF FACIAL RECOGNITION

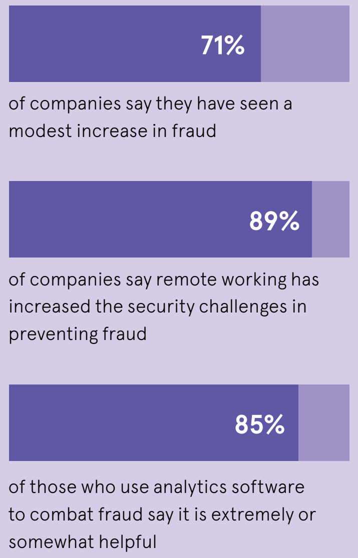
Consumers' responses to the question: "In which of these areas do you think the use of facial recognition technology should be restricted?"



Biometrics Institute, 2022

Commercial feature

THE PANDEMIC HAS SPURRED AN INCREASE IN FRAUD RISK



of companies say they have seen a modest increase in fraud

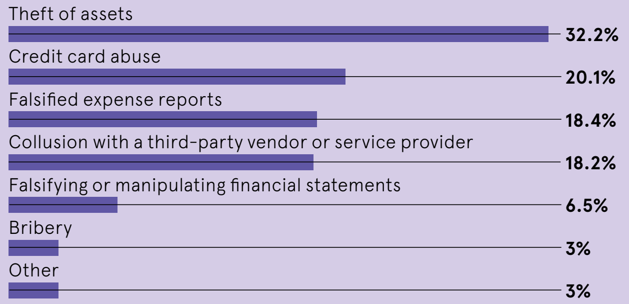
of companies say remote working has increased the security challenges in preventing fraud

of those who use analytics software to combat fraud say it is extremely or somewhat helpful

Caseware, 2022

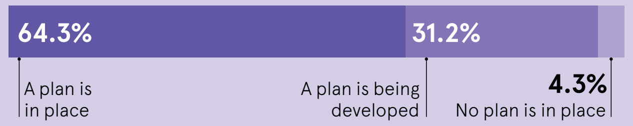
FRAUD RISKS COME FROM A NUMBER OF PLACES WITHIN AN ORGANISATION

The most concerning types of fraud



MANY ORGANISATIONS ARE LAGGING WHEN IT COMES TO FRAUD PREVENTION

The percentage of companies with a fraud prevention plan in place



Tackling the rise in online fraud

Data analytics is key to identifying and preventing fraud risk

Online fraud is on the rise. This has been exacerbated by the move to remote working due to the Covid-19 pandemic and a focus on balance sheets over security given the looming recession, leaving businesses more exposed to hackers than ever.

The consequences of fraud can be devastating, both financially and reputationally, costing companies billions of pounds a year, according to the UK's National Crime Agency.

The first step in the fight against fraud is to identify where the risk exists. That involves performing regular fraud risk assessments and implementing and enabling risk and compliance and/or internal audit functions within an organisation.

The rise in fraud is evidenced by Caseware's trends report 2022, which found that 71% of respondents had experienced a modest increase in fraud, while 35% did not have a fraud prevention and response plan.

The study revealed that 40% of respondents don't use or are unaware if their organisations use analytics software to mitigate fraud. Thus, it has never been more important for firms to protect themselves against the risk.

Companies also need to proactively carry out regular audits and management reviews to stay on top of the problem. Beyond that, they must create the appropriate channels for reporting fraud and investigating all those cases, as well as adopting technology which efficiently and effectively monitors for red flags.

Next, it's vital to establish a robust fraud prevention and response plan to stop it happening in the first place or, if it does occur, to stamp it out as soon as possible. By keeping up to date with the latest fraud trends, and continually raising awareness and promoting defence strategies throughout the company, the plan can be successfully executed.

"Businesses need buy-in from their employees to ensure successful implementation of the plan," says James Loughlin, head of data analytics at Caseware UK. "For starters, that means creating a positive culture and work environment in which everyone is pulling together in the same direction.

He adds: "Following on from that, companies must employ effective fraud prevention and detection strategies. They also need to invest not only in their IT, but employee training too, and take immediate action when an incident happens."

It's better to nip the problem in the bud before it escalates into something altogether more damaging to the business. That's why it's essential to implement and strengthen internal controls and apply clauses to contracts with external parties that allow them to be audited as necessary.

While technology plays a key role in tackling fraud, the software employed is only effective if it's correctly adopted by its users, therefore they must be fully trained on its use. Firms also need to ensure they update their technology as required to minimise the risk of fraud occurring through their core systems.

As a data analytics solutions provider, Caseware is at the forefront in combatting fraud. One of its solutions, Caseware IDEA, enables companies to detect, analyse and prevent fraud.

By focusing on areas and processes of the business with elevated risks and analysing large datasets to uncover every anomaly, the solution enables the user to quickly identify suspicious or fraudulent transactions. It also strengthens and monitors internal control effectiveness and provides more robust fraud risk coverage and assurance.

The integrated suite can be used to perform ad-hoc analyses of fraud investigations or automate analyses to create more responsive controls that better support risk management and, thus, prevent future issues. All these analyses are captured by Caseware IDEA and can therefore be used as evidence should legal proceedings be taken.

"By enabling customers to efficiently and effectively identify fraud and tackle it before it escalates, they can successfully mitigate the problem," says Scott Epstein, chief product officer at Caseware. "With online fraud becoming all too prevalent, it's, therefore, vital that companies have access to solutions which protect themselves against risk."

> Businesses need buy in from their employees to ensure successful implementation of the plan

For additional info on the software and the business, please also refer to caseware.co.uk/business/idea

caseware