# TechScape: Can the EU bring law and order to AI?

Publication Date: 2023-06-27

Author: Dan Milmo

Section: Technology

Tags: Technology, TechScape newsletter, Artificial intelligence (AI), European Union, European Commission, Computing, Europe, features

Article URL: https://www.theguardian.com/technology/2023/jun/27/techscape-european-union-ai

Deepfakes, facial recognition and existential threat: politicians, watchdogs and the public must confront daunting issues when it comes to regulating artificial intelligence. Tech regulation has a history of lagging the industry, with the the UK's online safety bill and the EU's Digital Services Act only just arriving almost two decades after the launch of Facebook. AI is streaking ahead as well. ChatGPT already has more than 100 million users, the pope is in a puffer jacket and an array of experts have warned that the AI race is getting out of control. But at least the European Union, as is often the case with tech, is making a start with the AI Act. In the US, senate majority leader Chuck Schumer has published a framework for developing AI regulations, one that prioritises goals like security, accountability and innovation – with an emphasis on the latter. In the UK, Rishi Sunak has convened a global summit on AI safety for the autumn. But the EU's AI Act, two years in the making, is the first serious attempt to regulate the technology. Under the act, AI systems are classified according to the risk they pose to users: unacceptable risk; high risk; limited risk; and minimal or no risk. They are then regulated accordingly. The higher the risk – the more regulation. The EU is blunt about systems posing an "unacceptable risk": they will be banned. Unacceptable risk includes systems that manipulate people, with the EU citing the rather dystopian example of voice-activated toys that encourage dangerous behaviour in children; "social scoring", or governments classifying people based on socio-economic status or personal characteristics (to avoid scenarios like in Rongcheng, China, where the city rated aspects of residents' behaviour). It also includes predictive policing systems based on profiling, location or past criminal behaviour; and biometric identification systems, such as real-time facial recognition. High-risk AI systems are those that "negatively affect safety or fundamental rights". They will be assessed before being put on the market, and will be checked while they're in use. The high-risk category includes systems used in education (like scoring of exams); operation of critical infrastructure; law enforcement (such as evaluating the reliability of evidence); and management of asylum, migration and border control. It also includes systems used in products that fall under the EU's product safety legislation such as toys, cars and medical devices. (Critics argue that the time and money it takes to comply with such rules may be daunting for start-ups in particular.) Limited risk systems will have to comply with "minimal transparency requirements" and users should be made aware of when they are interacting with AI, including systems that generate image, audio or video content like deepfakes. The EU parliament cites specific proposals for generative AI (tools like ChatGPT and Midjourney that produce plausible text and images in response to human prompts). AI-generated content will have to be flagged in some way (the EU wants Google and Facebook to start doing this straightaway). And AI firms will have to publish summaries of the copyrighted data used for training up these AI systems (we're still largely in the dark about this). Minimal or no risk systems, such as AI used in video games or spam filters, will have no additional obligations under the act. The European Commission says the "vast majority" of AI systems used in the EU fall into this category. Breaches of the act could be punished by fines of €30m or 6% of global turnover. (Microsoft, for instance, reported revenue of $198bn last year.) Risky business As existential fears about such technology's rapid rise abound and tech giants compete in an AI arms race, governments are beginning to seriously consider the warnings about AI and questions it raises, as my colleague Alex Hern and I reported on last week. The new EU AI act, meanwhile, addresses similar questions. What will it do about foundation models? Foundation models underpin generative AI tools like ChatGPT and are trained on vast amounts of data. The European parliament draft will require services like ChatGPT to register the sources of all the data used to "train" the machine. To combat the high risk of copyright infringement, the legislation will oblige developers of AI chatbots to publish all the works of scientists, musicians, illustrators, photographers and journalists used to train them. They will also have to prove that everything they did to train the machine complied with the law. They add that "deployers" of the systems should have human oversight and redress procedures in place for those tools. This also includes carrying out a "fundamental rights impact assessment" before the system is put in use. When will it become law and what is the "Brussels effect"? The EU is hoping to agree the final draft by the end of the year after MEPs voted in mid-June to push through an amended version of the draft originally tabled by the European commission. There are now trilateral talks between the commission, the EU parliament's AI committee chairs and the Council of the European Union to finesse the legislation. Lisa O'Carroll is the Guardian's Brussels correspondent, and she has been following the act closely. Lisa told me that real-time facial recognition, banned under the MEP proposals, will be a contentious issue, noting that: "Police forces and interior ministries see real-time facial recognition as an important tool in the fight against crime and some civil offences. This type of AI is already in force in parts of China, where drivers are watched for speeding, use of mobile phone or dozing off at the wheel." She added: "And the French government is – controversially – planning to use real-time AI facial recognition at next summer's Olympics to avert any potential threats such as crowd surges. Dragoş Tudorache, the co-rapporteur of the MEPs' AI committee, confirmed this law would have to be reversed if the AI act were in place. "The EU is hoping, once again, its regulation will become the 'gold standard' for some of the most significant players with the likes of Google and Facebook simply adopting the new laws as their operational framework globally. This is known as the 'Brussels effect'." Is the regulation likely to be influential? Charlotte Walker-Osborn, a technology lawyer specialising in AI, says the EU is influential in tech regulation globally – with laws like GDPR – and the AI Act will carry weight. But other countries like the US, UK and China are already looking to introduce their own measures, which will mean additional work for tech firms, businesses and other entities that fall within its scope. "Undoubtedly, there will be much additional and differing legislation outside of the EU bloc which companies will need to grapple with," she says. "While the EU act will, in many ways, set the bar, it is clear that a number of countries outside the European Union are drafting their own novel requirements, which companies will also need to grapple with." What do the critics say? Dame Wendy Hall, Regius Professor of computer science at the University of Southampton, says there is an alternative to the EU's risk-focused angle, such as the pro-innovation approach in a UK government white paper in March. "Although there has been some criticism of the UK approach not having enough teeth, I am much more sympathetic to that approach than the EU's," she said. "We need to understand how to build responsible, trustworthy, safe AI, but it's far too early in the AI development cycle for us to know definitively how to regulate it," she says. What do companies think? Sam Altman, the chief executive of OpenAI, the US company behind ChatGPT, has said the company will "cease operating" in the EU if it cannot comply with the act, although he publicly supported the notion of audits and safety tests for high-capability AI models. Microsoft, a major financial backer of OpenAI, believes that AI "requires legislative guardrails" and "alignment efforts at an international level," and has welcomed moves to get the AI Act implemented. Google DeepMind, the UK-based AI arm of the search giant, says it is important that the act "supports AI innovation in the EU". However, a paper published by researchers at Stanford University warned that the likes of Google, OpenAI and Facebook owner Meta are "especially poor" in doing things like summarising copyrighted data in their models. "We find that foundation model providers unevenly comply with the stated requirements of the draft EU AI Act," the researchers said. If you want to read the complete version of the newsletter please subscribe to receive TechScape in your inbox every Tuesday.