04 May 2021 | 17:25 GMT

Too Perilous For AI? EU Proposes Risk-Based Rules

Draft regulations splits AI applications into risk-based tiers and bans some

By **Lucas Laursen**

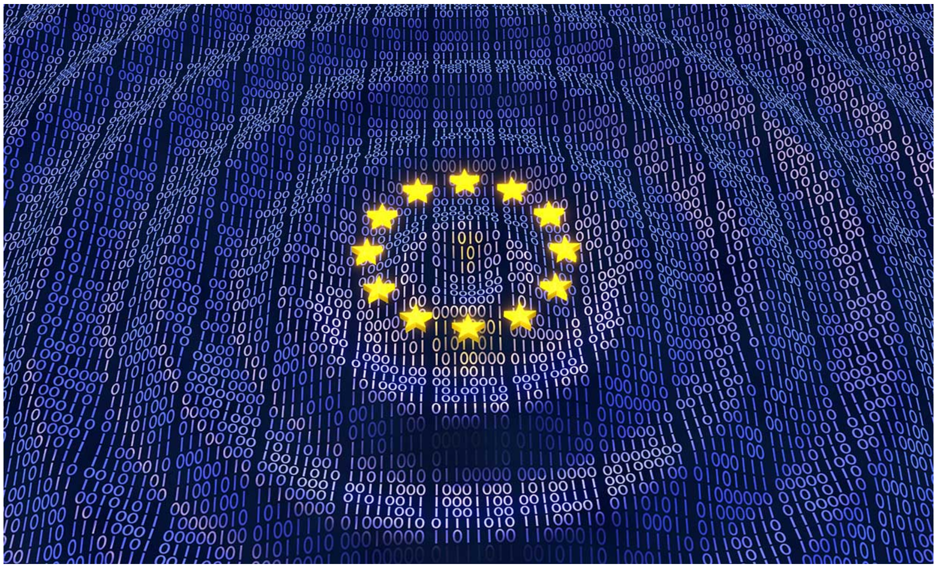

Illustration: iStockphoto

As part of its emerging role as a global regulatory watchdog, the European Commission published a proposal on 21 April for regulations to govern artificial intelligence use in the European Union.

The economic stakes are high: the Commission predicts European public and private investment in AI reaching €20 billion a year this decade, and that was before the additional earmark of up to €134 billion earmarked for digital transitions in Europe's Covid-19 pandemic recovery fund, some of which the Commission presumes will fund AI, too. Add to that counting investments in AI outside the EU but which target EU residents, since these rules will apply to any use of AI in the EU, not just by EU-based companies or governments.

Things aren't going to change overnight: the EU's AI rules proposal is the result of three years of work by bureaucrats, industry experts, and public consultations and must go through the European Parliament—which requested it—before it can become law. EU member states then often take years to transpose EU-level regulations into their national legal codes.

The proposal defines four tiers for AI-related activity and differing levels of oversight for each. The first tier is *unacceptable risk*: some AI uses would be banned outright in public spaces, with specific exceptions granted by national laws and subject to additional oversight and stricter logging and human oversight. The to-be-banned AI activity that has probably garnered the most attention is real-time remote biometric identification, i.e. facial recognition. The proposal also bans subliminal behavior modification and social scoring applications. The proposal suggests fines of up to 6 percent of commercial violators' global annual revenue.

The proposal next defines a *high-risk* category, determined by the purpose of the system and the potential and probability of harm. Examples listed in the proposal include job recruiting, credit checks, and the justice system. The rules would require such AI applications to use high-quality datasets, document their traceability, share information with users, and account for human oversight. The EU would create a central registry of such systems under the proposed rules and require approval before deployment.

Limited-risk activities, such as the use of chatbots or deepfakes on a website, will have less oversight but will require a warning label, to allow users to opt in or out. Then finally there is a tier for applications judged to present *minimal risk*.

As often happens when governments propose dense new rulebooks (this one is 108 pages), the initial reactions from industry and civil society groups seem to be more about the existence and reach of industry oversight than the specific content of the rules. One tech-funded think tank told the Wall Street Journal that it could become "infeasible to build AI in Europe." In turn, privacy-focused civil society groups such as European Digital Rights (EDRi) said in a statement that the "regulation allows too wide a scope for self-regulation by companies."

"I think one of the ideas behind this piece of regulation was trying to balance risk and get people excited about AI and regain trust," says Lisa-Maria Neudert, AI governance researcher at the University of Oxford, England, and the Weizenbaum Institut in Berlin, Germany. A 2019 Lloyds Register Foundation poll found that the global public is about evenly split between fear and excitement about AI.

"I can imagine it might help if you have an experienced large legal team," to help with compliance, Neudert says, and it may be "a difficult balance to strike" between rules that remain startup-friendly and succeed in reining in mega-corporations.

AI researchers Mona Sloane and Andrea Renda write in VentureBeat that the rules are weaker on monitoring of how AI plays out after approval and launch, neglecting "a crucial feature of AI-related risk: that it is pervasive, and it is emergent, often evolving in unpredictable ways after it has been developed and deployed."

Europe has already been learning from the impact its sweeping 2018 General Data Protection Regulation (GDPR) had on global tech and privacy. Yes, some outside websites still serve Europeans a page telling them the website owners can't be bothered to comply with GDPR, so Europeans can't see any content. But most have found a way to adapt in order to reach this unified market of 448 million people.

“I don’t think we should generalize [from GDPR to the proposed AI rules], but it’s fair to assume that such a big piece of legislation will have effects beyond the EU,” Neudert says. It will be easier for legislators in other places to follow a template than to replicate the EU’s heavy investment in research, community engagement, and rule-writing.

While tech companies and their industry groups may grumble about the need to comply with the incipient AI rules, Register columnist Rupert Goodwin suggests they’d be better off focusing on forming the industry groups that will shape the implementation and enforcement of the rules in the future: “You may already be in one of the industry organizations for AI ethics or assessment; if not, then consider them the seeds from which influence will grow.”

About the Tech Talk blog

IEEE Spectrum’s general technology blog, featuring news, analysis, and opinions about engineering, consumer electronics, and technology and society, from the editorial staff and freelance contributors.

Follow @IEEESpectrum Subscribe to RSS Feed

x