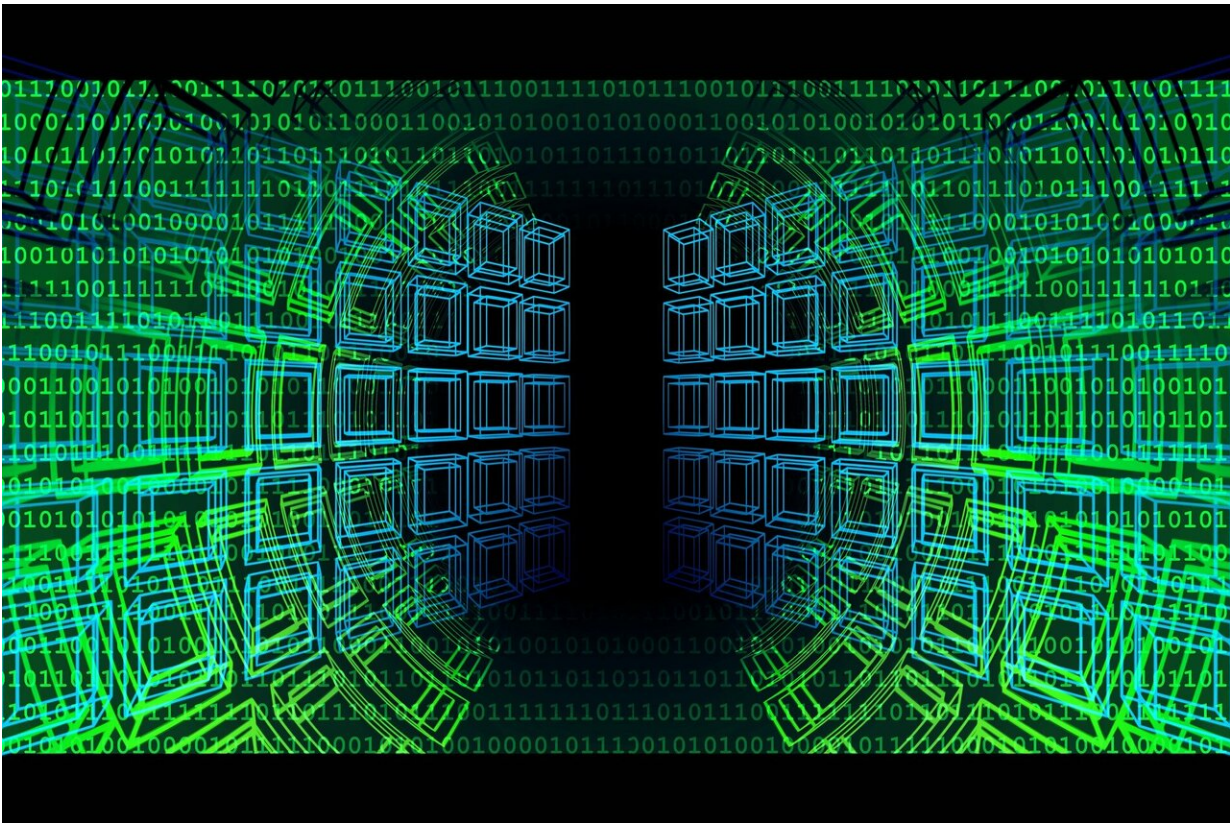# The world is finally starting to regulate artificial intelligence—what to expect from US, EU and China's new laws

November 15 2023, by Alina Patelli

Credit: CC0 Public Domain

Most mainstream applications of artificial intelligence (AI) make use of its ability to crunch large volumes of data, detecting patterns and trends

within. The results can help predict the future behavior of financial markets and city traffic, and even assist doctors to diagnose disease before symptoms appear.

But AI can also be used to compromise the privacy of our online data, automate away people's jobs and undermine democratic elections by [flooding social media with disinformation](). Algorithms may [inherit biases from the real-world data]() used to improve them, which could cause, for example, discrimination during hiring.

AI regulation is a comprehensive set of rules prescribing how this technology should be developed and used to address its potential harms. Here are some of the main efforts to do this and how they differ.

The EU AI act and Bletchley Declaration

[The European Commission's AI Act]() aims to mitigate potential perils, while encouraging entrepreneurship and innovation in AI. The [UK's AI Safety Institute](), announced at the recent government summit at Bletchley Park, also aims to strike this balance.

The EU's act bans AI tools deemed to carry unacceptable risks. This category includes products for "social scoring", where people are classified based on their behavior, and real-time facial recognition.

The act also heavily restricts high-risk AI, the next category down. This label covers applications that can negatively affect fundamental rights, including safety.

Examples include autonomous driving and AI recommendation systems used in hiring processes, law enforcement and education. Many of these tools will have to be registered in an EU database. The limited risk category covers chatbots such as ChatGPT or image generators such as

Dall-E.

Across the board, AI developers will have to guarantee the privacy of all personal data used to "train"—or improve—their algorithms and be transparent about how their technology works. One of the act's key drawbacks, however, is that it was developed mainly by technocrats, without extensive public involvement.

Unlike the AI Act, the recent Bletchley Declaration is not a regulatory framework per se, but a call to develop one through international collaboration. The 2023 AI Safety Summit, which produced the declaration, was hailed as a diplomatic breakthrough because it got the world's political, commercial and scientific communities to agree on a joint plan which echoes the EU act.

The US and China

Companies from North America (particularly the US) and China dominate the commercial AI landscape. Most of their European head offices are based in the UK.

The US and China are vying for a foothold in the regulatory arena. US president Joe Biden recently issued an executive order requiring AI manufacturers to provide the federal government with an assessment of their applications' vulnerability to cyber-attacks, the data used to train and test the AI and its' performance measurements.

The US executive order puts incentives in place to promote innovation and competition by attracting international talent. It mandates setting up educational programs to develop AI skills within the US workforce. It also allocates state funding to partnerships between government and private companies.

Risks such as discrimination caused by the use of AI in hiring, mortgage applications and court sentencing are addressed by requiring the heads of US executive departments to publish guidance. This would set out how federal authorities should oversee the use of AI in those fields.

[Chinese AI regulations](#) reveal a considerable interest in generative AI and protections against deep fakes (synthetically produced images and videos that mimic the appearance and voice of real people but convey events that never happened).

There is also a sharp focus on regulating AI recommendation systems. This refers to algorithms that analyze people's online activity to determine which content, including advertisements, to put at the top of their feeds.

To protect the public against recommendations that are deemed unsound or emotionally harmful, Chinese regulations ban fake news and prevent companies from applying dynamic pricing (setting higher premiums for essential services based on mining personal data). They also mandate that all automated decision making should be transparent to those it affects.

The way forward

Regulatory efforts are influenced by national contexts, such as the US's concern about cyber-defense, China's stronghold on the private sector and the EU's and the UK's attempts to balance innovation support with risk mitigation. In their attempts at promoting ethical, safe and trustworthy AI, the world's frameworks face similar challenges.

Some definitions of key terminology are vague and reflect the input of a small group of influential stakeholders. The general public has been underrepresented in the process.

Policymakers need to be cautious regarding tech companies' significant political capital. It is vital to <u>involve them in regulatory discussions</u>, but it would be naive to trust these powerful lobbyists to police themselves.

AI is making its way into the fabric of the economy, informing financial investments, underpinning national health care and social services and influencing our entertainment preferences. So, whomever sets the dominant <u>regulatory framework</u> also has the ability to shift the global balance of power.

Important issues remain unaddressed. In the case of job automation, for instance, conventional wisdom would suggest that digital apprenticeships and other forms of retraining will transform the workforce into data scientists and AI programmers. But many highly skilled people may not be interested in software development.

As the world tackles the risks and opportunities posed by AI, there are positive steps we can take to ensure the responsible development and use of this technology. To support innovation, newly developed AI systems could start off in the high-risk category—as defined by the EU AI Act—and be demoted to lower risk categories as we explore their effects.

Policymakers could also learn from highly regulated industries, such as drug and nuclear. They are not directly analogous to AI, but many of the quality standards and operational procedures governing these safety-critical areas of the economy could offer useful insight.

Finally, collaboration between all those affected by AI is essential. Shaping the rules should not be left to the technocrats alone. The <u>general public</u> need a say over a technology which can have profound effects on their personal and professional lives.

Citation: The world is finally starting to regulate artificial intelligence—what to expect from US, EU and China's new laws (2023, November 15) retrieved 27 April 2024 from https://techxplore.com/news/2023-11-world-artificial-intelligencewhat-eu-china.html