Over the past few months, efforts to regulate artificial intelligence have heated up in Europe, North America, and Asia, both at the national and local levels. We discussed the implications for companies of this increasingly complex regulatory environment with Steven Mills, BCG’s chief AI ethics officer, and Kirsten Rulf, a partner and the firm’s associate director for data and digitalization.

MEET STEVEN AND KIRSTEN
BCG: What’s behind the recent flurry of AI regulatory moves?

Steven Mills: AI regulations have been in the works for a number of years. But the sudden arrival of generative AI tools like ChatGPT created new urgency. Governments are responding to heightened concern among the general public about AI. In Europe, which is about to enact the Artificial Intelligence Act after years of debate, there is also political pressure on leaders who have staked their careers on regulating AI. The challenge for governments is how to regulate AI without stifling innovation.

What does the EU’s AI Act call for?

Kirsten Rulf: The draft of the AI Act does three things. First, it establishes a definition of AI. Next, it lays out a risk framework, defining use cases that present unacceptable risk, high risk, limited risk, or little or no risk. Finally, it enables enforcement by establishing implications if companies fail to adhere to requirements—including fines of up to 6% of global annual revenue.

AI systems posing unacceptable risk will be prohibited. Use cases that fall in the “high risk” category are those that could unintentionally cause emotional, financial, or physical harm. For example, they could influence access to social-service benefits, housing, credit, health care, or employment. The AI Act will lay out a set of requirements, including disclosure, certification, transparency, and postdeployment documentation for these use cases.

What comes next?

Rulf: Now that the European Parliament and the council of member states have stated their positions on the EU Commission’s original draft, all three entities will negotiate on the final law. A lot can still happen in these talks. While the law’s basic framework is likely to stand, the specific use cases that fall within each risk category, and when and how foundational models will be included, will continue to evolve.

The EU Parliament and council of member states must then vote on a final draft, possibly in mid-fall 2023 but almost certainly by the end of the year. After that, there will likely be a grace period of one or
two years before the law goes into effect. Individual member states are likely to adopt it into law very quickly, well before it becomes mandatory for the entire EU.

Regulatory compliance will require solutions that are integrated into a company's broader AI technology stack.

The AI Act, moreover, isn't coming out in a vacuum. In the EU, there is also the Data Act, the Cybersecurity Act, and the Digital Services Act, which regulates online platforms. Then there is the General Data Protection Regulation (GDPR), which went into effect in 2018. A recent study counted 104 European laws on digital technologies and data. Companies face an increasingly complex regulatory compliance challenge that will require solutions that are integrated as part of their broader AI technology stack. This complexity could come at a big upfront cost and requires time to implement.

What’s happening in the US?

Mills: At the national level, US AI regulation is nascent. Several proposals are before Congress, but there’s been no indication that they will move forward. US states and cities are beginning to act, however, with laws passed in California, Illinois, New York City, and elsewhere. In the absence of national-level regulation, we expect federal agencies to apply existing regulatory regimes to AI, consistent with prior White House guidance. The Federal Trade Commission, Consumer Financial Protection Bureau, and others have already issued statements implying this strategy. A patchwork of AI regulation is beginning to emerge as a result.

This sounds like quite a regulatory jungle. What will this mean for companies deploying AI globally?

Mills: Companies will need to determine which regulations apply in each jurisdiction in which they operate and ensure they comply. Note that it may depend on where the AI model is built, not just where it will be used. My big fear is that companies will overlay all of these regulations and end up with something that is far, far more restrictive than what any one jurisdiction imagined or intended. This has the potential to stifle AI use.

What’s the chance that the EU laws will become the de facto global standard?

Rulf: I don’t think all countries will follow the EU regulatory framework. But it’s clear from the discussions in the US, Europe, and around the world that regulations are coming. So I think many
global companies will just implement the EU AI Act as a first framework while their own regulators keep working. In effect, therefore, it could become a de facto standard for companies. I can only see that happening, however, if the EU can communicate and implement the law in a way that companies can actually operationalize without stifling innovation. The EU would have to put out very clear standards explaining how you can build an AI product and make it safe. Otherwise, it will take a long time for companies to decipher the regulatory language into something that can be implemented.

**How could vague or poorly written policy stifle a good use of AI?**

**Rulf:** Let’s use a health care example. From a policymaker’s standpoint, it makes total sense to subject all use of AI in health care to stringent disclosure and transparency requirements. Now imagine a company wants to use generative AI to make it easier for doctors to prepare an exit memo summarizing patient treatment and postrelease care. A simple, easy-to-understand memo would be useful for patients, who may otherwise go home and search the internet to interpret a diagnosis and get advice on posttreatment care. This type of summarization is well within generative AI capabilities today. And because it inherently includes doctor input, there is a human in the loop. But under emerging regulation, it may be considered high risk, creating a regulatory burden that makes pursing this use case too costly.

Some companies will continue to pursue high-risk use cases, of course, because they know AI can deliver an incredibly positive impact and because they have the right responsible AI programs in place. But many companies may walk away, saying, “I’m not going to do anything high risk—period. It’s just not worth it.”

**Is it too late for companies to influence the regulatory details?**

**Rulf:** In Europe, where regulation is furthest along, it’s too late to influence the basic framework. But there’s still time for companies to give input on the details to EU policymakers and to legislators and regulators in the member states. In the US, as Steve mentioned, the whole process is just starting.

**Mills:** Policymakers should continue getting the perspective of the big tech companies, who continue to innovate and develop many of the foundational models, as they did recently when seven US tech companies committed to voluntary safeguards. The group that isn’t being consulted enough, though, is the 99% of companies who will be implementing AI. These companies also need to be in the dialogue and have a voice. They need to explain to policymakers what is going to be realistic and achievable from a regulatory standpoint. If the requirements are too onerous, it could become impossible for the average, nontech company to deploy AI.

**How well prepared are companies for emerging AI regulations?**

**Mills:** Many tech companies are well positioned. They deeply understand the technology and have responsible AI teams in place. It’s the other 99% of companies—those that will be implementing AI models—that need to take steps to prepare. Too many are waiting until new AI regulations actually go into effect.
These companies don't realize that the fundamental process and basic steps that need to be in place are clear. For example, creating good documentation of the AI systems. The specific details of what needs to be included may change, but the broad-brush requirements are already understood.

**Rulf:** I think European companies are much less prepared than those in the US. We saw the same with the EU’s data-protection regulations. Many companies didn't get into the details of compliance until it was too late. About a week before the GDPR went into effect in 2018, many European companies were still scrambling. Our hope is that by raising these issues now, we can encourage companies to avoid the same type of scramble this time.

**Assuming they have a basic responsible AI program, how can companies proceed using generative AI in high-risk areas?**

**Rulf:** If you really look at the process of doing a high-risk use case, it is not really any different with generative AI relative to other types of AI. You need to have somebody shepherd the product from the moment of conception to the moment of certification, and then have somebody watch over it once it’s deployed. And document each step of the process, the risks that were identified, the steps taken to mitigate them, and how you validated mitigation.

**What’s your advice to companies that aren’t prepared at all?**

**Mills:** Start setting up a responsible AI program now because it takes an average of about three years to get there. You really need an agile and holistic responsible AI framework that encompasses strategy, processes, governance, and tools. You will need to communicate this transformation throughout your organization. First movers in all this will have a big advantage. If you have an adaptable framework, there will be cost up front. But it’s the only way you will be able to leverage AI to the fullest over the long term.

**ABOUT BOSTON CONSULTING GROUP**

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.