

The Potential Impact of the European Commission's Proposed AI Act on SMEs

The use of artificial intelligence (AI) technology has been consistently growing in popularity; therefore, many countries are designing and implementing policy frameworks to address the use of AI with regard to its ethical and security-related impacts.¹ These frameworks can have far-reaching effects, both positive and negative. One example of a proposed framework is the European Commission Artificial Intelligence Act (AI Act) of 2021, which could have significant impacts on small and medium-sized enterprises (SMEs).

The Need for AI Regulation

The use of AI has tremendous potential for organizations because it makes it possible to extract results from huge amounts of data and create new business models. AI will potentially increase economic output by US\$13 trillion.² However, AI can also create risk for individuals, organizations and society at large (figure 1).³ This includes both the intentional malicious use of AI by individuals, organizations and governments for their own purposes (e.g., cyberattacks, precision propaganda, autonomous weapons)⁴ and unintentional damage due to sophisticated software delivering unwanted outcomes (e.g., social media algorithms pointing to increasingly extreme content to keep consumers engaged).⁵ As a result, AI can influence human behavior, make discriminating decisions, damage financial systems and promote political instability.

Proposed AI Act

To cope with these challenges and to minimize AI-related threats, the European Commission has proposed regulations on AI use. In the proposed AI Act, the European Commission defines AI as “machine learning approaches, including supervised, unsupervised and reinforcement learning,” and “logic- and knowledge-based approaches” and “statistical approaches.”⁶ AI systems are divided into three groups of risk: unacceptable risk, high risk and low risk (figure 2). The European Commission proposes to prohibit unacceptable-risk algorithms; closely monitor, impose restrictions on and require documentation for high-risk algorithms; and establish significantly fewer requirements for low-risk algorithms.



JAKOB GASSAUER

Is an undergraduate student at Ludwigshafen University of Business and Society (Ludwigshafen, Germany) in a cooperative study program with BASF SE, a global chemical enterprise. He has completed internships in various departments, such as corporate development and the digitalization unit of BASF's agrochemical business. His research interests include the digitalization strategies of the manufacturing industry.

GERALD F. BURCH | PH.D.

Is an assistant professor at the University of West Florida (Pensacola, Florida, USA). He teaches courses in information systems and business analytics at both the graduate and undergraduate levels. His research has been published in the *ISACA® Journal*. He can be reached at gburch@uwf.edu.

FIGURE 1
AI Threats

Individuals	Organizations	Society
<ul style="list-style-type: none"> Physical safety Privacy and reputation Digital safety Financial health Equity and fair treatment 	<ul style="list-style-type: none"> Financial performance Nonfinancial performance Legal and compliance Reputational integrity 	<ul style="list-style-type: none"> National security Economic stability Political stability Infrastructure integrity

The European Commission has also set forth guidance to punish individuals and enterprises that fail to comply with the regulations. The highest fines—up to €30 million or 6 percent of global revenue (whichever is higher)—could be imposed for using prohibited systems and violating regulations applicable to high-risk systems. Less serious violations could result in fines up to €20 million or 4 percent of global revenue (whichever is higher). Even the use of incorrect information or the provision of misleading information to authorities could lead to fines of €10 million or 2 percent of global revenue.⁷

The proposed law also includes significant administrative requirements associated with AI implementation. High-risk AI systems would be subject to transparency requirements. These include risk management systems, data governance and management, record keeping and logging, transparency and user access to information, human

oversight, accuracy, robustness and cybersecurity, a conformity assessment, post-market monitoring systems, and registration with EU member-state governments. In addition, the European Commission would require high-risk algorithms to maintain technical documentation, including a general description of the AI system, its purpose and impacts, the processes and methods by which the system was developed, and all the changes the system has undergone during its lifetime.

Research on governance of enterprise IT (GEIT) has shown that “firms often perceive governance and management investments for their information and related technology as costly and complex.”⁸ Therefore, organizations are placed in a position of determining the value of implementing AI and the cost and complexity associated with GEIT.

Potential Financial and Competitive Impact for SMEs

A study to support an impact assessment of the AI Act estimates that AI investments will grow from €16 billion in 2021 to approximately €66 billion in 2025.⁹ The study estimates that 17 percent of these investments will be needed to meet regulatory requirements, resulting in additional costs of €11.9 billion in 2025, shrinking the funds available for research into or application of AI technologies.¹⁰

FIGURE 2
AI System Classification

	Description	Proposed Implications
Unacceptable risk	<ul style="list-style-type: none"> Systems causing physical or psychological harm and exploiting vulnerabilities of a specific group Real-time remote biometric identification systems in publicly accessible spaces Systems that use all forms of social scoring 	<ul style="list-style-type: none"> Unacceptable-risk AI systems will be prohibited
High risk	Systems for: <ul style="list-style-type: none"> Biometric identification and categorization of natural persons Management and operation of critical infrastructure such as water, gas, heating and traffic Educational and vocational training Employment, workforce management and access to self-employment Access to and enjoyment of essential private services and public services and benefits Law enforcement Migration, asylum and border management Administration of justice and democratic processes 	Implementation of and Requirement for: <ul style="list-style-type: none"> Risk management system Data governance and management Technical documentation Record keeping and logging Transparency and provision of information to users Human oversight Accuracy, robustness and cybersecurity Conformity assessment Registration with EU member-state government Postmarket monitoring system
Low risk	<ul style="list-style-type: none"> Systems such as chatbots, AI-enabled video and computer games, spam filters and most other low impact AI systems 	<ul style="list-style-type: none"> Fewer and less complex requirements such as notifications when interacting with a machine

Additional costs will arise if enterprises offer products or services in high-risk AI sectors. The combined costs of implementing and using AI may be a substantial problem for SMEs that have fewer resources (e.g., legal staff, monetary funds) than big enterprises. Based on the EU's impact assessment, for a small enterprise with up to 100 employees or €10 million in turnover, and without a functioning quality management system, the initial costs of incorporating AI into its processes could be up to €400,000.¹¹ Assuming the average profit margin of 10 percent for SMEs, the enterprise would have negative profits if it implemented an AI system.

A common way for organizations to evaluate their competitive advantage is to take a resource-based view of their organization. The resource-based model developed by US academic Jay Barney, Ph.D., states that enterprises use available resources to create capabilities to gain a competitive advantage.¹² **Figure 3** shows how SMEs implementing AI in an environment governed by the proposed European Commission AI Act could determine whether using AI would become a competitive advantage for their enterprise.

This model shows that SMEs with a small, or no, legal staff may not have the necessary resources to create or use AI capabilities. As a result, these enterprises may not build a competitive advantage and will have a

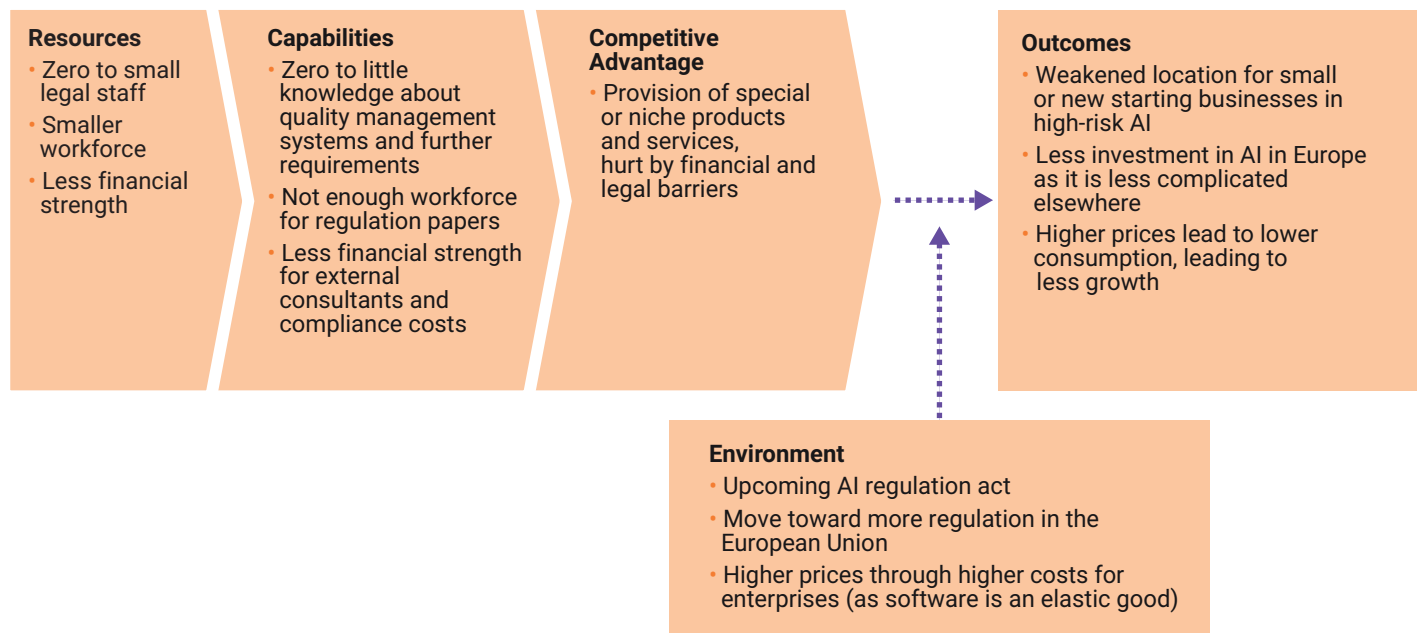
weaker market position than larger enterprises. In this case, the European Commission's proposed AI Act might create an unfavorable environment for SMEs.

What Can Be Done?

There is no doubt that governing bodies should address the fundamental rights and ethical standards associated with AI, including discrimination and bias, human oversight, data protection, civil society involvement and societal impacts.¹³ At issue is how to ensure that organizations, especially SMEs, are not negatively affected.

Possible solutions may be to change the definition of AI. An assessment of the AI Act shows there are concerns from practitioners that the definition is too broad.¹⁴ This may create situations in which organizations may have to limit their use, governance or range of potential AI-related activities. In contrast, the same assessment shows that academics and nongovernmental organizations think the current AI definition is too narrow and more items should be added. Another concern about the current AI Act definition is the binary classification of high vs. low risk. Many feel this approach is too simplified and that a larger spectrum of categories may reduce some of the issues associated with forcing certain AI practices into

FIGURE 3
Resource-Based Model for SMEs Using AI



What was once thought of as an opportunity for SMEs to compete with larger enterprises through the effective use of technology may be undone by government regulations that favor larger enterprises with more resources.

the high-risk category because they are not low risk.¹⁵ Therefore, adjusting the definition of AI may allow SMEs to determine the type of AI they can afford to consider.

A second useful approach for SMEs is to require less oversight or create offices inside governing organizations to ensure that compliance issues are being addressed.¹⁶ These offices could potentially help SMEs determine whether their AI choices require further governance and provide recommendations that may help them determine which AI practices align with their strategic goals.

Other options that may help SMEs stay compliant with the AI Act might come from software vendors or AI consulting firms that assist SMEs with considering their AI options and developing their AI Act compliance plans. This approach would add compliance costs, but SMEs might be able to share the expenses across enterprises rather than each enterprise absorbing its own costs.

It is likely that some form of the proposed AI Act will become law; therefore, changes will occur for all organizations using AI. For larger organizations, changes to their existing GEIT plans will be necessary. This will further increase the cost and complexity of these plans. Similarly, SMEs operating in the European Union should examine emerging AI-related risk and determine how to address the broader concerns of the AI Act. In addition, software and consulting enterprises must determine their potential liability if they help SMEs implement AI.

SMEs operating outside the European Union should continuously monitor what is happening in their own regions because many governing organizations are considering how to address AI concerns. These regulations, though well intentioned, stand to negatively affect the potential competitive advantage SMEs can gain through the use of AI. What was once thought of as an opportunity for SMEs to compete

with larger enterprises through the effective use of technology may be undone by government regulations that favor larger enterprises with more resources.

Conclusion

AI is an emerging technology that has demonstrated substantial benefits. It can make enterprises more effective and efficient, increase sales and decrease costs. However, like most new technologies, there are still many unknowns, and the world has yet to deal effectively with the legal, ethical and political components of AI.

The resource-based model indicates that AI regulation will affect the environment and alter the relationship between competitive advantage and output. Research estimates the cost of compliance with the AI Act will be between €1.6 billion and €3.3 billion and the certification process for AI products will increase development costs by 10 percent to 14 percent.¹⁷ Funding AI implementation and paying for government compliance may therefore erase the benefits of AI use for some organizations. The resource-based model shows that large organizations that have more financial resources may be able to absorb the costs of compliance and application certification to take advantage of the AI benefits and further increase their competitive advantage. However, SMEs may not have the resources to comply with the regulations and may lose any competitive advantage they once had.

The European Commission's proposed AI Act is one example of how regulating the use of AI can help protect individual rights. However, the cost to comply with government regulations can be prohibitive, especially to SMEs. The balancing act is to find definitions and regulations that address both concerns simultaneously.

It is likely that some form of regulation of AI systems in the European Union—and many other countries—will be implemented in the future. All enterprises, both inside and outside the European Union, should consider how such regulations might affect the way organizations can ethically use AI to increase their competitive advantages while still protecting individual rights. Special consideration should also be given to organization size and how government regulations may unfairly increase the competitive advantages of large organizations over smaller organizations.

Author's Note

The European Parliament Committees and Parliament plenary are scheduled to vote on the draft AI Act in February and March 2023. Following these votes, discussions between the EU Member States, Parliament and the European Commission are expected to begin in April 2023. The final AI Act could be adopted by the end of 2023.

Endnotes

- 1 Renda, A. et al.; *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe Final Report (D5)*, European Commission, Brussels, April 2021
- 2 Bughin, J.; J. Seong; J. Manyika; M. Chui; R. Joshi; "Notes From the AI Frontier: Modelling the Impact of AI on the World Economy," McKinsey Global Institute, 4 September 2018, <https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy>
- 3 Cheatham, B.; K. Javanmardian; H. Samandari; "Confronting the Risks of Artificial Intelligence," *McKinsey Quarterly*, 26 April 2019, <https://www.mckinsey.com/capabilities/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence>
- 4 Brundage, M. et al.; "The Malicious Use of Artificial Intelligence," Future of Humanity Institute, February 2018, <https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf>
- 5 Friedersdorf, C.; "YouTube Extremism and the Long Tail," *The Atlantic*, 12 March 2018, <https://www.theatlantic.com/politics/archive/2018/03/youtube-extremism-and-the-long-tail/555350/>
- 6 European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, Brussels, April 2021
- 7 *Ibid.*
- 8 De Haes, S.; A. Joshi; W. van Grembergen; "State and Impact of Governance of Enterprise IT in Organizations: Key Findings of an International Study," *ISACA® Journal*, vol. 4, 2015, <https://www.isaca.org/archives>
- 9 *Op cit* Renda
- 10 *Ibid.*
- 11 Center for Interfirm Comparison, *Benchmarking Report: Industry Overview 2016*, Association for Consultancy and Engineering, United Kingdom, 2016
- 12 Barney, J.; "Firm Resources and Sustained Competitive Advantage," *Journal of Management*, vol. 17, iss. 1, 1991, p. 99–120
- 13 Chatterjee, S.; "Impact of AI Regulation on Intention to Use Robots: From Citizens and Government Perspective," *International Journal of Intelligent Unmanned Systems*, December 2019, p.109–111
- 14 *Op cit* Renda
- 15 *Ibid.*
- 16 Smuha, N.; E. Ahmed-Rengers; A. Harkens; W. Li; J. MacLaren; R. Piselli; K. Yeung; "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act," LEADS Lab, University of Birmingham, Alabama, USA, August 2021
- 17 *Op cit* Renda



ENJOYING THIS ARTICLE?

- Learn more about, discuss and collaborate on emerging technology in ISACA's Online Forums. <https://engage.isaca.org/onlineforums>

An Enhanced Experience. Just One Login Away.

ISACA's updated Engage platform delivers an enhanced experience designed to foster greater connections, elevated discourse and a heightened sense of community. Plus, you'll stay up-to-date on the latest tech trends and insights with a brand new activity feed for a true social media feel.

Visit engage.isaca.org to start engaging on the next level with ISACA.

