COSMOS
Navigate the Compliance Universe

CEP Magazine - August 2022
The use of artificial intelligence: Ways to manage risks

By Kamal Hossain Meahzi

Kamal Hossain Meahzi (meahzi.law@gmail.com) is pursuing an advanced masters in compliance at the University of Fribourg, Switzerland, and a practicing lawyer of the Supreme Court of Bangladesh.

Kamal Hossain Meahzi

The use of artificial intelligence (AI) in business is rising at scale. Its use received further importance in the last two years due to the COVID-19 pandemic. With the increase of AI use in various sectors, both the associated benefits and risks are getting highlighted. Businesses must acknowledge these risks to redefine their compliance plan before using an AI system in their business. This article is an attempt to identify some risks related to the use of AI. Based on these risks, a compliance plan is suggested to mitigate and/or monitor risks related to using and implementing AI.

Benefits and risks of using AI

The use of AI is considered a substitute for human labor. Modern Al can enhance and replace tasks of human skill in the same manner that past machines replaced human muscles. AI is beneficial not only to industries but also for consumers. Benefits include the reduction of economic inefficiencies and labor costs, as well as an increase in high-skilled jobs. Moreover, AI can help companies understand their individual customers better and thus develop more customized products tailored to their specific needs. For consumers, AI has increased their choices of products. AI is being used in different sectors, such as transportation, education, manufacturing, media, healthcare, banking, etc. However, there are risks. Businesses interested in using AI should be familiar with these risks to redefine their compliance plan. The pertinent risks associated with the use of AI may be summarized as follows:

- **Discrimination and bias**: There is a concern that AI systems are sometimes discriminatory and fail to ensure fairness. AI-generated decisions are based on algorithms. Algorithmic bias might affect marginalized communities. For example, Amazon's AI recruiting model was found to be biased against women. Upon investigation, it was found that the system favored male job applicants.[1] The other issue of serious concern is that the rise of this technology has the potential to create a new form of discrimination—price discrimination. Price discrimination occurs when the same product is sold at different prices to a different group of customers, whereas the cost of production is same. Organizations might charge discriminatory prices by analyzing customer data and behavior.

- **Technical risks**: Software and hardware systems, which are at the root of AI-based decisions, are highly error-prone and susceptible to manipulation because of cyberattacks. For example, Germany's government network was successfully hacked.[2]

- **Privacy risks**: AI makes decisions using a large quantity of data. Access to data is fundamentally important to the development of digital technologies in general, and AI in particular. AI systems, if abused, will put the personal data of individuals and their privacy at risk.

Risk mitigation and monitoring

Because AI can expedite complex and time-consuming decisions, organizations are increasingly willing to use AI. Since the use of AI is closely connected with data rights, privacy rights, intellectual property protection, ethics, social values, and so on, it is necessary for an organization to have strategies in place to mitigate AI risks and monitor the system properly. It is also essential to remain vigilant about relevant AI policies, rules, regulations, and legislation for ensuring algorithmic fairness, transparency, and accountability.

- **Data protection**: As AI uses data and produced outcomes based on large amounts of data, keeping it safe should be a priority. "The key risks when using AI or machine learning tools in the deal environment are around data security," said Stephen Bates, partner at KPMG.[3] From a European perspective, data protection is a fundamental right guaranteed by article 8 of the European Union Charter of Fundamental Rights. As such, using an AI system requires a thorough understanding of privacy and data protection laws. For example, the General Data Protection Regulation (GDPR) in Europe includes nondiscrimination requirements for algorithmic profiling and a right to obtain an explanation of automated decisions that significantly affect users. So the AI principles framed by the company should cover all aspects relevant for AI systems (e.g., safety, data privacy, security, fairness). Most AI-related incidents are unintended side effects of the technology, such as bias and lack of explanation. Companies need to be cautious about the incidents that might occur while using the system. Under GDPR, a data protection impact assessment (DPIA) is necessary while processing certain categories of data, for instance, a systematic and extensive evaluation of the personal aspects of an individual, including profiling, processing of sensitive data on a large scale, systematic monitoring of public areas on a large scale, etc. A DPIA is mandatory if similar data is used in an AI system.

- **Cybersecurity**: As mentioned earlier, software and hardware are susceptible to manipulation by cyberattack. No system in the world is breach-proof. However, since AI means using software and hardware to perform certain tasks, industry-standard security should be used to protect the system from attack. For example, the National Institute of Standards and Technology Cybersecurity Framework may be followed. This framework looks at cybersecurity from beginning to end. It may be used as a guide to implement cybersecurity. It requires the identification of cybersecurity resources, the protection of those resources, the detection of unauthorized access, responding to unauthorized access, and system recovery the system.

- **Corporate governance**: The concept of modern corporate governance requires businesses to take into account the well-being of all stakeholders. Stakeholders include employees, consumers, suppliers, banks, investors, local community, government, environment, etc. Proper monitoring should be in place to verify that AI-based decisions are not making biased decisions.

- **Human rights due diligence**: The use of AI should not come into conflict with human rights. The right to equality and freedom from discrimination are two basic human rights guaranteed by national and international human rights instruments. Absent the use of AI, no human is permitted to act in violation of a basic human right. Monitoring of the AI system by a human being is essential so that its use does not result in human rights violations, and that such violations can be immediately remediated upon discovery.

Jeanne Boillet, EY global innovation leader and a member of the EY Global Assurance Executive Committee, has formulated certain questions for considerations by the board. In an article, Boillet emphasized that the board should understand the potential impact of AI on the organization's business model, culture, strategy, and sector:[4]

- How is the board challenging management to respond strategically to both the opportunities presented by AI and the risks associated with it?
- How is the organization using AI technology and new data sets for governance and risk management?
- Does the organization have a talent strategy for recruiting and retaining people with the necessary skillsets to manage and staff AI-related projects?
- Has the board asked management to assess how the adoption of AI impacts the integrity of its finance function or its financial statements?

The quest for answers to these questions may help organizations use AI systems more effectively, efficiently, and ethically.

Takeaways

- Artificial intelligence (AI) is an autonomous system. It makes decisions through a self-learning process, meaning AI is not an instrument but a decision-maker.
- The use of AI benefits both industry and consumers.
- AI does not exist in a vacuum. The use of AI relates to the issues of human rights, privacy rights, intellectual property rights, and so on.
- There are risks when using AI, including technical risks, the breach of privacy rights, and the violation of human rights.
- AI systems should ensure the protection of human rights and be technically safe, ethically sound, and socially beneficial.

[1] Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women," Reuters, October 10, 2018,https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.
[2] Birgit Jennen, "Pro-Russian Hackers Hit German Government Sites, Spiegel Says," Bloomberg, May 6, 2022, https://www.bloomberg.com/news/articles/2022-05-06/german-government-sites-hit-by-pro-russian-hackers-spiegel-says.
[3] Sam Shaw, "The risks of AI and how to mitigate them," Institute of Chartered Accountants in England and Wales, accessed June 7, 2022, https://www.icaew.com/insights/features/2020/mar-2020/the-risks-of-ai-and-how-to-mitigate-them.
[4] Jeanne Boillet, "Why AI is both a risk and a way to manage risk," EY, April 1, 2018, https://www.ey.com/en_gl/assurance/why-ai-is-both-a-risk-and-a-way-to-manage-risk.