Publication date:
15 May 2019
Author:
Sandeep Sukhavasi
Analyst

Evolving Global AI Policies and Regulations

Brought to you by Informa Tech

Table of Contents:

Table of Figures:

Summary

In brief

Artificial intelligence (AI) as a concept and technology is still in a nascent stage of development, but is evolving more rapidly than anticipated. Several countries worldwide have already announced AI as part of their national technology strategy, while a few more have begun the public consultation process. Despite these, the regulation of AI has not been keeping up pace with the developments, with several regulators taking an ex-post approach and ensuring a technology-neutral approach and developing ethics, privacy, and security guidelines. The evolving developments of AI will disrupt the existing conventional business models and create new roles and opportunities. Furthermore, governments and policy-makers will need to amend existing policies and regulatory frameworks to enable the seamless integration and adoption of AI.

The initial AI regulatory approaches of the EU, Japan, US, UK, and Singapore are included in this report.

Ovum view

- **Regulators are currently taking an ex-post approach rather than an ex-ante one:** AI is still in an early development and adoption phase. Due to the lack of clarity around the disruption that AI is expected to cause to existing business models, regulators and governments worldwide have chosen to issue technology-neutral guidelines. This allows greater flexibility as the technology develops. With policy-makers currently preferring to take an ex-post approach, more industry-specific and established frameworks are expected to evolve over time to complement these guidelines.
- **Guidelines issued are primarily focused on protecting fundamental rights:** While governments across several countries are taking steps to introduce regulatory frameworks for AI, the majority of interim guidelines issued so far are focused on protecting fundamental rights such as ethics, privacy, and security. To introduce effective frameworks, policy-makers and stakeholders across the AI value chain should work in tandem. Eventually, the aim should be to create policies and regulations that touch all aspects of AI.
- **AI will create new opportunities and governments should be prepared to seize those:** AI already has a comprehensive range of applications across various industries and is disrupting existing business models with new approaches. While this is considered a threat by some, if instead AI is embraced, new opportunities across industries and the value chain can be created, including new technical and administrative roles. To ensure such opportunities are utilized, governments should allocate funds to up-skill the workforce and citizens. Furthermore, governments can set up AI boards to advise respective government ministries on the opportunities arising from adopting AI and help them set out roadmaps for a coordinated government approach and for reskilling the workforce.
- **Governments will need to amend existing regulations to accommodate AI:** While governments are still working to publish regulatory policies and guidelines for AI, there are several regulations that are

already in place to safeguard consumer interest and competition. To ensure the smooth integration of AI across various industries, regulators would need to revisit and amend several of these existing, and in some cases outdated, regulations. This is especially true in areas where there is a conflict of interest between AI applications and existing policies, such as data protection laws, outdated user consent methods, licensing agreements or permits, and sector-specific laws.

Current state of play

AI – the dawn of a new era

The term AI is very generic, and its attributes will differ based on the application and deployment. For a better understanding, AI can be classified as "AI software" and "AI agent."

AI software refers to programs that have the ability to learn and improve through experiences and adjust their programs or algorithms to handle similar or new scenarios based on past experiences. The AI software learns through the data that it is fed directly by users, through a repository of data that it is connected to, or through interactions with the external environment such as sensors. Machine learning (ML) and deep learning (DL) programs are part of the AI software.

AI agents are devices into which the AI software is integrated. The AI agents can act as a hosting platform to the AI software, such as cloud services to which other AI agents or non-AI agents are networked, or can be agents that physically interact with the outer environment through actuators or displays such as robots and machinery.

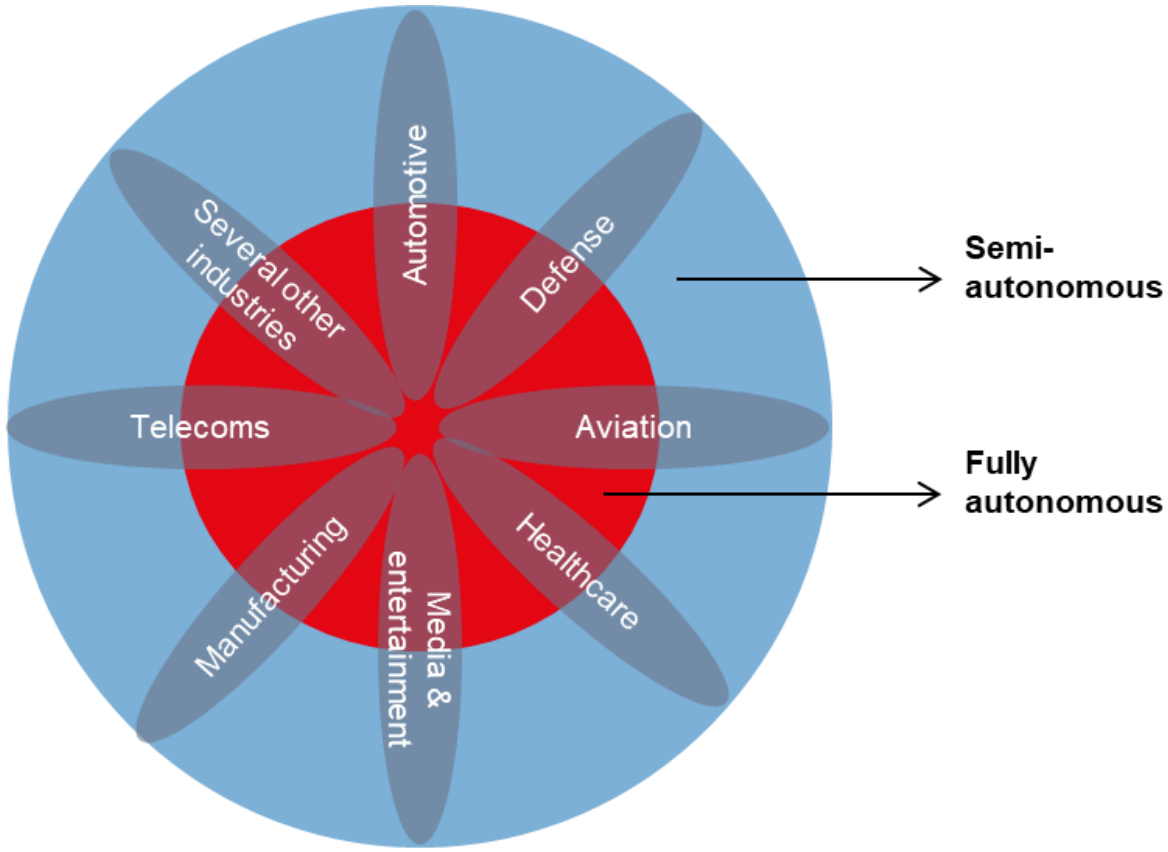
Both AI software and AI agents can be categorized into fully autonomous and semi-autonomous segments respectively. Collectively or independently, the AI software and AI agent have found various applications across several industries ranging from automotive, aviation, and defense, through to healthcare, consumer electronics, and more.

The current developments and deployments of AI are still in the early stages. While a few AI systems are fully autonomous, the majority of these are still supervised and controlled using human interference. In time, and with further advancements, the human supervision and interference will reduce, paving the way to a greater number of AI applications that are completely autonomous.

Figure 1 gives an indication of some of the industries where AI could have an application. This includes industries that can be fully or semi-automatized, such as automotive, healthcare, and manufacturing.

Figure 1: Overview of industries where AI could have an application

Figure 1: Overview of industries where AI could have an application1



The necessity for regulations in AI

Technology adoption has become an inevitable part of a human's life and its advancements have become crucial for betterment. The adoption of new technologies often spurs debate among groups that support and oppose the implementation. AI has its own fair share of debates too, except that it seems the voices of these groups are louder, and concerns are far greater, than other emerging technologies. Approving the adoption of a certain technology just because it has gained adequate support, or discarding it due to a fear of opposition, are not considered good practice for policy-makers. It is the duty of the government and policy-makers to diligently weigh up the risks and benefits of the technology before arriving at an opinion.

While it is too early to lay down stringent rules to regulate AI, several countries worldwide have already initiated efforts through public consultations and discussions with policy-makers, academics, and corporations. Ovum believes that imposing early regulations on emerging technologies would choke innovations and investments, while a delay would lead to competition crisis and antitrust motions, and force companies into legal trouble due to regulatory uncertainty. The governments and policy advisors should focus on establishing basic guidelines and policies initially, and introduce ex-ante policies in general.

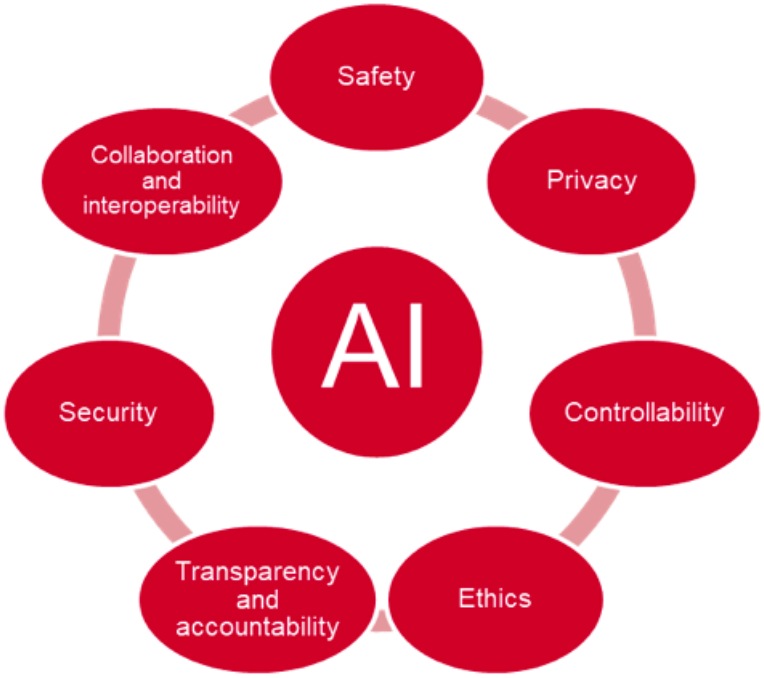
Ex-post and more matured industry-specific regulations can be framed at a later stage, depending on the application of AI in the respective sectors.

Regulatory challenges of AI and Ovum's take

Ovum has identified seven key AI regulation challenges, as shown in Figure 2.

Figure 2: Regulatory challenges of AI

Figure 2: Regulatory challenges of AI2



Safety

Safety is the most basic feature that any government considers while approving the deployment of, not just AI, but any machinery or technology that directly or indirectly poses threat to life or property, or that causes economic or financial losses. The threat is exponentially higher in the case of AI, due to its ability to act independently and with minimal human interference. Imposing safety standards on AI software is just as important as imposing them on AI agents. Policy-makers will need to take special interest in framing safety standards in areas that directly or indirectly involve a greater threat to life or property from deployment of AI, such as aviation, transportation, mining, logistics, and defense. In the near future, it would not be surprising if governments set up a safety board or agency and obligated companies to get safety approval from these authorized entities to permit the deployment of AI.

Privacy

AI decisions are shaped based on the underlying data and its algorithms, which are designed to evolve over time with experience. The greater the amount of data, the easier it will be for the AI to make meaningful patterns and emulate human behavior. However, gaining access to useful data has raised privacy concerns across the world, with most countries already rolling out data protection laws such as the General Data Protection Regulation (GDPR). Furthermore, provisions in data protection laws that mandate data controllers and data processors to disclose the purpose of data collection and its usage will pose a big challenge, as this cannot be clearly defined while it is being fed to AI applications. The gradual adoption of AI will eventually force governments and policy-makers to revisit data protection measures to make amendments to the existing data protection laws, to ensure a trade-off between protecting users' privacy and data collection.

Controllability

The current developments and deployments of AI are still in the early stages. While a few AI systems are fully autonomous, the majority of these are still supervised and controlled using human interference. In time, and with further advancements, the human supervision and interference will reduce, paving the way to a greater number of AI applications that are completely autonomous. However, the failure of such systems due to external factors such as exposure to unfamiliar scenarios, a breach in security, or damage to components and sensors, or internal factors such as software malfunctions and inefficiently trained systems, would result in greater damage, especially across industries that involve critical decision-making, such as aviation, automotive, defense, and healthcare. The policy-makers should enforce a controllability code within AI applications that will enable humans to take control of the system during a time of uncertainty. Furthermore, the controllability will enable human interference in cases where the AI system deviates from its intended duties that it was designed to perform or when it identifies that a certain task is outside of its limits. In parallel, efforts on controlling the data fed in to train the AI system will help to develop a trustworthy system.

Ethics

Ethics plays the most pivotal role in shaping regulatory policies on AI, with several governments across the world already incorporating an ethics code as part of their national strategies. Since the development and training of an AI system is a continuous process that involves developing algorithms and feeding in data, as well as monitoring and updating the system, policy-makers should be extra cautious about defining the ethical guidelines. The guidelines should help avoid unfair biasness, prevent the input of inappropriate data to train AI systems, and maintain respect for privacy, developing AI systems with an undisclosed agenda on which the very fundamentals of the AI applications would be built.

Developing a trustworthy and robust AI system will involve multiple professional stakeholders, such as developers, statisticians, academics, and data cleansers. The policy-makers and governments should work alongside each other to invest and train professionals to incorporate the best ethical practices in their AI systems. Arguably, this is not something that is new to governments as many already allocate a considerable amount of funds toward training citizens to improve digital skills as part of their respective national plans. Also, in future, it is expected that AI companies will choose to introduce a new AI ethics officer role, or even an AI ethics board, to monitor and safeguard ethical values being incorporated into the AI systems, similar to a data protection officer.

Transparency and accountability

For a system to be trustworthy, transparency plays a crucial role, and with the involvement of AI systems that not only collect data but also make decisions, the AI companies must be even more cautious in gaining the trust of consumers, even in sectors where there are no stringent regulatory measures. Therefore, policy designers must ensure that, as far as possible, AI companies are transparent both fundamentally and technically.

Fundamental transparency

Fundamentally, the regulator should mandate that an AI system must disclose its identity beforehand and should empower users with the right to reject the interaction and obligate provisions through other modes of communication. Furthermore, the regulator should obligate AI systems to disclose information about any data that they intend to collect or have already collected and divulge the purpose of this data collection to users in the interest of users' privacy, especially in scenarios where the users are under AI surveillance.

Technical transparency

Technically, policy-makers should make provisions in the regulations to obligate AI companies to make their AI systems as transparent as possible; these include algorithms and any reasoning behind why and how the AI system has arrived at a certain decision, especially when it is created for public use. However, policy-makers should ensure they strike a balance between maintaining transparency and corporate interests. This is because imposing heavy transparency obligations could create challenges for AI companies when it comes to protecting their intellectual property and could deter progress in the sector.

Although concerns around collecting and safeguarding data are already addressed under existing data protection laws in respective countries, amending the existing laws to accommodate AI systems and improve transparency will help the government to hold the entity or developer accountable.

Security

AI will thrive only when the users are confident that their information is secure, and that the systems are not easily vulnerable to threats. The threat is even more sophisticated if the data that is fed into the AI system for learning is hacked and the AI system is misled. For AI systems to be secure, the companies should ensure, not just physical security, but security of the system across the entire value chain, from networks and data to software. Although building a secured AI system is more of a concern to the company developing it than just the regulators, policy-makers should look to set technical standards, such as encryption standards for storing data and cybersecurity controls to prevent unauthorized access.

Furthermore, policy-makers can define certification standards that the companies need to fulfill to ensure that the AI system is secure, both physically and internally, for commercial deployments. These can cover:

- robustness
- respective industry board standards
- technical standards (more so when the AI system is for public use).

Over the period of AI system deployment growth across the industries, policy-makers can introduce more refined industry-specific standards to gain the trust of users.

Collaboration and interoperability

Development and adoption of an AI ecosystem is still in a nascent stage. For society to embrace new technology, there must be a collaborative approach between various stakeholders, including private sector, government, academics, and citizens. Governments and policy-makers together should foster the development of the necessary infrastructure and establish common platforms to share research and data to develop inclusive AI models that address the various needs of both private and public entities. Also, governments should create a roadmap to train and educate citizens to embrace the adoption of novel technologies such as AI.

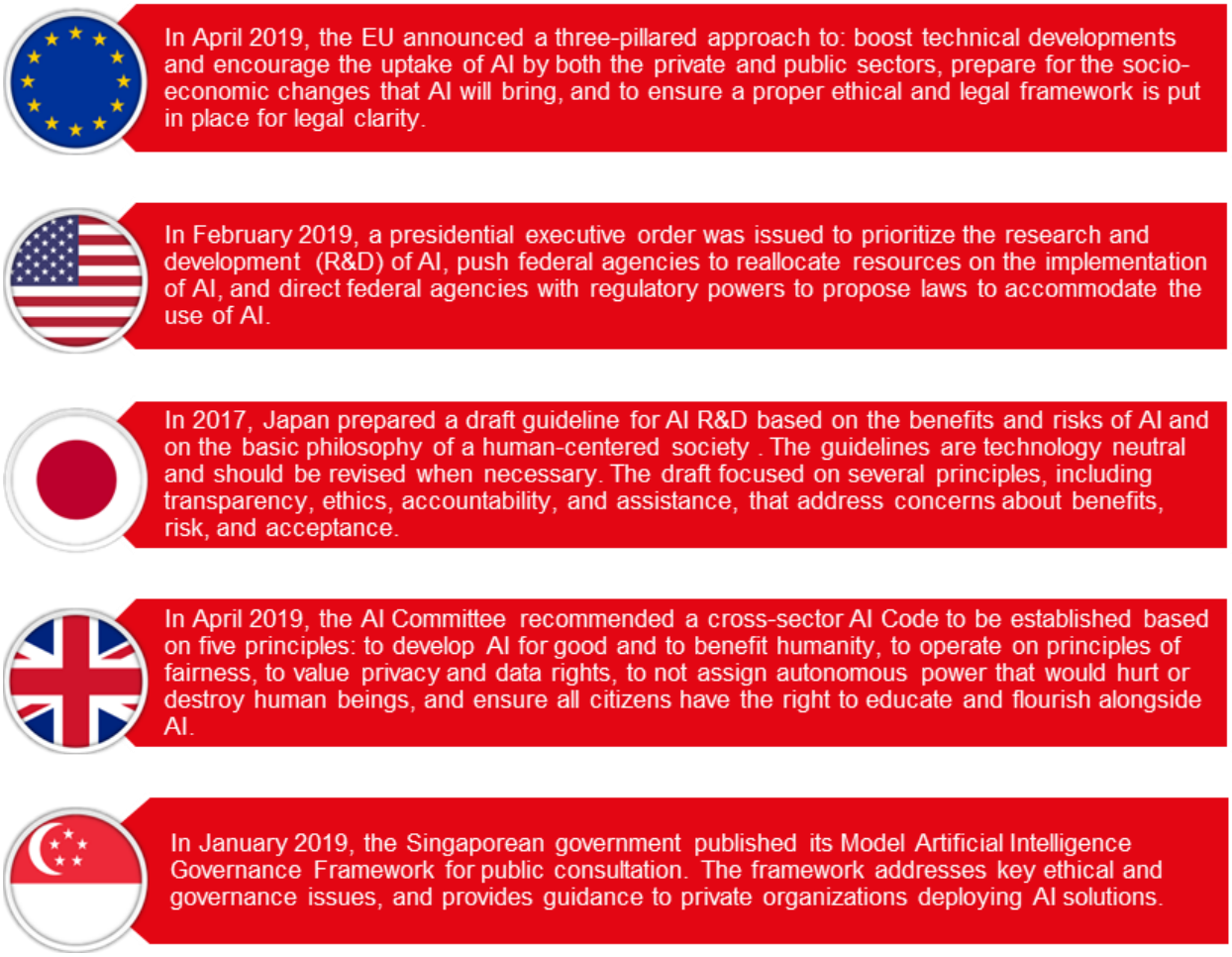
Furthermore, with the AI ecosystem still in the early stages of development, to avoid dominance of a particular entity, which would set off anti-trust concerns, policy-makers should focus on establishing standard, internationally accepted protocols. An open interface should be created to ensure that there is fair practice regarding interoperability between AI systems that should be followed by all developers and entities. Also, the rise of AI systems will pave the way for new business models and increase the number of applications for new patents. To support these changing needs, respective government departments and policy-makers should set policies and licensing terms collaboratively to ensure a smooth transition.

Major global developments in AI regulation

In this section, Ovum looks at the initial AI regulatory approaches of the EU, Japan, US, UK, and Singapore, as shown in Figure 3.

Figure 3: AI regulation strategies

Figure 3: AI regulation strategies3



European Union

The European Commission (EC) has articulated a coordinated EU approach to adopting and promoting the development of AI. It has encouraged cooperation between member states to address any challenges

brought about by AI. In April 2018, the EU member states and Norway inked a cooperation commitment to work together on AI. The EC has announced an EU approach based on three pillars:

- boosting technical developments and encouraging the uptake of AI by both the private and public sectors
- preparing for the socio-economic changes that AI will bring
- ensuring a proper ethical and legal framework is put in place for legal clarity.

As part of setting up an ethical and legal framework, the EC has focused on addressing issues related to GDPR to build trust and to ensure legal clarity is communicated to the stakeholders. The EC has formed a High-Level Experts Group (HLEG) on AI that will support the implementation of the EU strategy on AI. Additionally, HLEG will recommend policy developments on ethical, legal, and social issues associated with AI. In December 2018, HLEG issued its first draft on AI ethics guidelines, in which it assessed a broad range of factors that are required to develop trustworthy AI.

The final version of HLEG's AI ethics guidelines was issued in April 2019, in which it gave seven key recommendations for trustworthy AI systems to fulfill, including:

- robustness and safety
- transparency
- privacy and data governance
- fairness
- accountability
- human agency and oversight
- societal and environmental well being.

The expert group will run a pilot phase of these recommendations and will gather feedback from the pilot phase, which will be presented to the EC in early 2020.

US

In 2016, the Democratic administration created a taskforce to provide recommendations on AI to the federal agencies and other actors. The taskforce issued two reports in October 2016 and December 2016, respectively. In the first report, the taskforce recommended the establishment of a Subcommittee on Machine Learning and Artificial Intelligence, which represents over 18 federal departments and agencies, and aims to coordinate and share knowledge and best practices about ML and AI.

The report also detailed policy recommendations and the approach needed to regulate AI. The taskforce concluded that, since AI can be incorporated into several products that are already subject to regulations to protect the end users, regulators should study how the existing regulations will be affected due to the incorporation of AI. It recommended that policy-makers introduce new regulations where the existing regulations fail to protect the end users due to the introduction of AI, and ensure that the policy-makers take into consideration the cost of complying with the new regulations.

In February 2018, the Subcommittee on Information Technology under the House Committee on Oversight and Government Reform held hearings on AI and recommended that federal agencies review federal

privacy laws and regulations to understand if these need to be updated to accommodate AI. Furthermore, it added that AI algorithms that make decisions about people should be made accountable and reviewable.

In February 2019, the US President, Donald Trump, passed an executive order to prioritize the research and development of AI. The order also pushes federal agencies to reallocate resources and present an annual plan on the implementation of AI in their respective departments, and directs federal agencies with regulatory powers to propose laws to accommodate the use of AI. No deadline for the annual plan has been set.

Japan

In 2016, Japan hosted the G7 summit, during which the Japanese Ministry of Internal Affairs and Communication proposed to create principles of AI development to promote the benefits of AI, mitigate risks, and improve acceptance of the new technology, which the G7 countries all agreed to. The G7 countries held discussions over the AI R&D principles and guidelines that were put forward by the Japanese ministry. Considering the international discussion, in 2017, Japan prepared draft guidelines for AI R&D based on the benefits and risks of AI and on the basic philosophy of a human-centered society. The guidelines are technology neutral and should be revised when necessary. The draft focused on several principles, including transparency, ethics, accountability, and assistance, addressing concerns on benefits, risk, and acceptance.

Also in 2016, the Japanese government issued Japan's Society 5.0 to create a super-smart society for providing customized solutions by adopting technologies such as AI, robotics, big data, and IoT. With this, Japan is set to introduce amendments to its existing laws and roll out new policies to accommodate technologies such as AI and robots in the near future. However, no amendments had been made at the time of writing.

UK

The UK's Industry Strategy

In November 2017, the UK government published the Industry Strategy announcing plans to develop industries of the future, and has put AI and the data revolution at the forefront. As part of the strategy, the government has set up a Centre for Data Ethics and Innovation, an advisory body to review the current landscape and advise the government on how to maximize the benefits of data-enabled technologies, including AI. Furthermore, the government has established an AI Council to coordinate and grow AI in the UK. The AI Council will take the leadership role by bringing in academia and industry experts across the sector to promote the adoption of AI across all sectors of the economy and will be supported by the Government Office for AI, which is a joint unit between the Business Growth Directorate in the Department for Business, Energy & Industrial Strategy and the Digital & Tech Policy Directorate in the Department for Digital, Culture, Media and Sport (DCMS).

Appointing a Select Committee on AI

In June 2017, the Select Committee on AI was appointed by the House of Lords to assess the implications of AI. The committee published its final report in April 2018, in which it recommended a cross-sector AI Code to be established based on five principles:

- to develop AI for good and to benefit humanity
- to operate on principles of fairness

- to value privacy and data rights
- to not assign autonomous power that would hurt or destroy human beings
- to ensure all citizens have the right to educate and flourish alongside AI.

Additionally, the report included other recommendations, such as:

- avoiding the monopolization of data by big technology companies
- providing greater control over personal data
- ensuring transparency in using AI
- making AI part of the curriculum in primary education
- needing a national policy framework
- reskilling and training the workforce to mitigate the effect of AI on jobs
- creating a framework for sharing data for healthcare
- turning academic work into commercial potential
- investing in AI development.

Establishing a Ministerial Working Group on Future Regulation

In June 2018, the UK government responded to the House of Lords and confirmed that it agreed with its recommendations. Furthermore, the government has committed to invest in innovative and knowledge-intensive businesses, including AI, and allocate funds to reskill and educate citizens. The government also plans to establish a Ministerial Working Group on Future Regulation to scan the horizon and identify areas where regulations would be needed to support emerging technologies such as AI. For this, the government plans to establish a £10m Regulators' Pioneer Fund to support regulators developing new approaches to handling emerging technologies such as AI.

Singapore

In April 2018, the Monetary Authority of Singapore (MAS) created a working committee to set principles for promoting the use of AI and data analytics, primarily for the financial sector. The Fairness, Ethics, Accountability and Transparency (FEAT) Committee was joined by several representatives from over 35 reputable financial organizations and institutions. In November 2018, MAS, in coordination with the FEAT committee, introduced a set of generally accepted principles, such as justifiability, accuracy and bias, ethics, internal and external accountability, and transparency for the use of AI and data analytics in decision making to firms offering financial products and services.

In January 2019, the Singaporean government published its Model Artificial Intelligence Governance Framework for public consultation. The framework addresses key ethical and governance issues and provides guidance to private organizations deploying AI solutions. The guidelines underpinning the model should help organizations realize that AI solutions are human centric and that the decisions made by AI should be fair, transparent, and reasonable. The model will be piloted by businesses and the feedback generated by the pilot will be used to further fine-tune the framework. Singapore will also collaborate with the World Economic Forum's (WEF's) center to drive AI and data innovation. Singapore's regulatory

authority, Infocomm Media Development Authority (IMDA), and the WEF will be involving organizations to discuss the Model Framework in detail and to enable its adoption.

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com