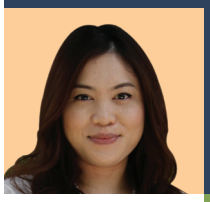
Artificial Intelligence: The European Approach and Beyond



by Eleena Abd Wahab

On 21 April 2021, the European Commission (**EC**) adopted a proposal for a harmonising set of rules for artificial intelligence systems (**AI Systems**), putting forth proposed legislation for a "*coordinated European approach to the human and ethical implications*" of artificial intelligence (**AI**).[1] The objectives behind the EC's 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[2] (**Proposed Regulation**) appear to be two-pronged: to give users the confidence to embrace AI-based solutions while also encouraging businesses to develop AI.[3] Ultimately, the Proposed Regulation is aimed at establishing a framework that will enable the European Union (**EU**) to be a global leader in the development of secure, trustworthy and ethical AI.

Overview of Proposed Regulation

1. Framework

The core elements of the Proposed Regulation are as follows:[4]

(a) harmonising rules for the placing on the market, the putting into service and the use of AI Systems in the EU;

(b) prohibition of certain AI practices;

(c) specific requirements for high-risk AI systems and obligations for operators of such systems;

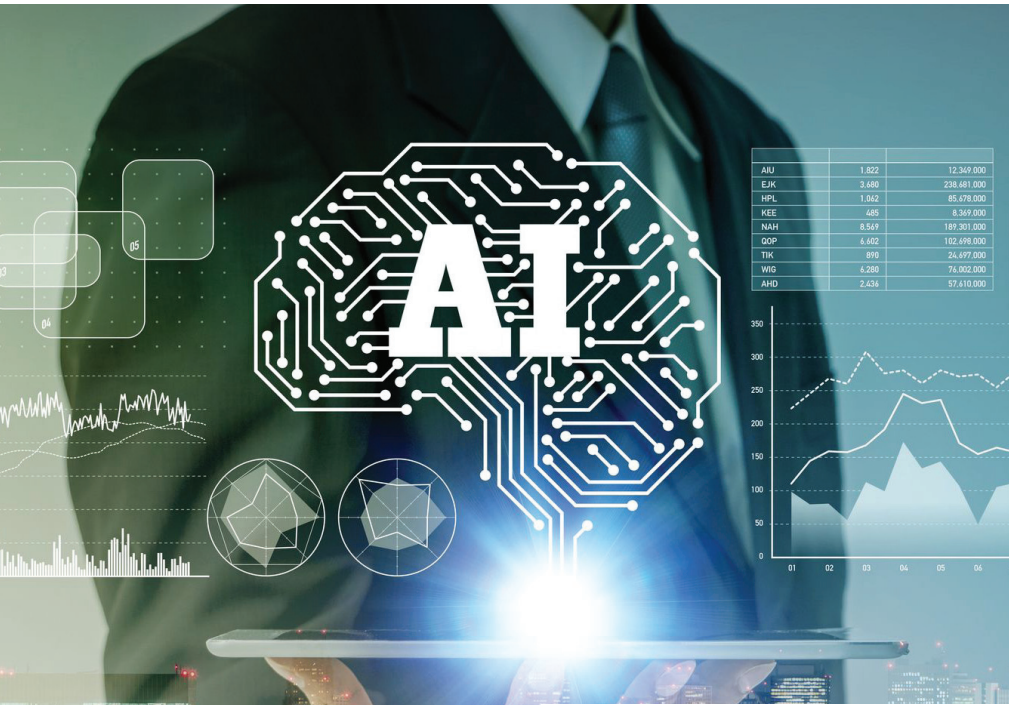
(d) harmonised transparency rules for AI Systems intended to interact with natural persons, emotion recognition systems and biometric categorisation

1 Proposal for a Regulation of the European Parliament and the Council, Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, p 1, available at https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF and the Annexes to the Proposed Regulations available at https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF

2 Available at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

3 Proposed Regulation, at p 1

4 Article 1, Proposed Regulation



systems, and AI Systems used to generate or manipulate image, audio or video content; and

(e) rules on market monitoring and surveillance.

"AI Systems" are broadly defined as all software developed with techniques and approaches such as machine learning approaches, logic and knowledge-based approaches, and statistical approaches.[5]

2. *Applicability of Proposed Regulation and extraterritorial effect*

The Proposed Regulation will apply to providers placing AI on the market or putting into service AI Systems in the EU, irrespective of whether those providers are established in the EU or in a third country.[6] Additionally, providers and users of AI systems located in a third country will also be governed by the Proposed Regulation if the output produced by the AI System is used in the EU.[7] Interestingly, the Proposed Regulation will not apply to public authorities in a third country, or organisations in a third country where the AI systems are used within the context of international law enforcement and judicial cooperation with the EU, or a Member State.[8]

3. *Prohibited AI practices*

The Proposed Regulation sets out a number of prohibited AI Systems which the EC has deemed as unacceptably risky due to the contravention of EU values and violation of fundamental rights. The prohibited AI Systems include:[9]

(a) AI Systems that utilise subminimal techniques beyond a person's consciousness to materially distort a person's behaviour in a manner that causes physical or psychological harm;

(b) AI Systems that exploit the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes physical or psychological harm;

(c) AI Systems by public authorities used for the evaluation of natural persons over a certain period of time based on their social behaviour or known or characteristics, leading to the detrimental or unfavourable treatment of certain natural persons in social contexts unrelated to the context in which the data was originally generated or collected; or the detrimental or unfavourable treatment of certain natural persons that is unjustified; and

(d) AI Systems that use "real-time" remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless necessary and in specific circumstances.

4. *High-risk AI Systems*

Providers of certain AI Systems which are categorised as high-

5 Article 3, Proposed Regulation
6 Article 2, Proposed Regulation
7 *Ibid*
8 *Ibid*
9 Article 5, Proposed Regulation

risk pursuant to the Proposed Regulation are required to adhere to specific requirements such as, among others, ensuring transparency in the design and development of the high-risk AI Systems;[10] ensuring that there is human oversight of the AI System to reduce risks to health, safety and fundamental rights;[11] establishing a risk management system throughout the lifetime of the high-risk AI System to analyse risks and adopt risk management measures and deploying a high level of accuracy, robustness and security throughout the lifecycle of the high-risk AI System;[12] and establishing a post-market monitoring system to monitor the performance of the high-risk AI System throughout their lifetime.[13]

AI Systems qualify as high-risk if it is intended to be used as a safety component of a product, or is itself a product falling within the purview of specific product safety legislation specified in Annex II of the Proposed Regulation; or standalone AI Systems which the use of may create an impact on health, safety and fundamental rights as referred to in Annex III. This includes AI Systems used in specific areas such as, among others, biometric identification and categorisation of natural persons, management and operation of critical infrastructure, education and vocational training, employment and law enforcement.[14]

Certain obligations are also imposed on the users of high-risk AI.[15]

5. *Non-high-risk AI Systems*

Non-high-risk AI Systems are regulated less stringently under the Proposed Regulation. Certain non-high-risk AI Systems are required to comply with transparency obligations, that is, to ensure that individuals interacting with the AI System are aware that they are interacting with an AI System and to disclose that the AI System may carry out emotion recognition or biometric categorisation or when the content has been manipulated or artificially generated.[16]

6. *Establishment of a regulatory authority*

The Proposed Regulation provides for the establishment of a regulatory body to monitor and advise the EC on matters under the Proposed Regulation, known as the European Artificial Intelligence Board.[17] As a result of this, Member States are required to have competent national authorities to oversee the domestic implementation of the Proposed Regulation.[18]

7. *Sanctions*

A contravention of the Proposed Regulation is punishable by monetary sanctions of up to EUR30 million or up to 6% of the global annual turnover, whichever is higher.[19]

The Proposed Regulation is only one of the key elements in the EU's holistic approach to AI. The EC also published a Coordinated Plan of Artificial Intelligence[20] to ensure a collective commitment by the Member States in maximising Europe's potential to lead in the field of AI. The EC also has plans to invest EUR1 billion per year in AI and has set a target of up to EUR20 billion per year in AI investments.[21]

The Proposed Regulation is currently under consideration by the Council of the EU.

AI in Malaysia

According to the Government AI Readiness Index published by the International Research Development Centre and Oxford Insights,[22] Malaysia is ranked 28th out of 172 countries in respect of the government's readiness to adopt and implement AI in the delivery of public services to its citizens, specifically within the healthcare, education and transportation sectors. In October 2017, the then government announced the development of the National

10 Article 13, Proposed Regulation
11 Article 14, Proposed Regulation
12 Article 9, Proposed Regulation
13 Article 61, Proposed Regulation
14 Article 6, Proposed Regulation
15 Articles 28 and 29, Proposed Regulation
16 Article 52, Proposed Regulation
17 Article 56, Proposed Regulation
18 Article 59, Proposed Regulation
19 Article 71, Proposed Regulation
20 Available at https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review
21 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, pp 1-2, available at https://digital-strategy.ec.europa.eu/en/library/communication-fostering-european-approach-artificial-intelligence
22 Available at https://www.oxfordinsights.com/government-ai-readiness-index-2020

Artificial Intelligence Framework (**NAIF**) spearheaded by the Malaysia Digital Economy Corporation Sdn Bhd (**MDEC**). Previously set to be launched by end of 2019, NAIF has yet to be finalised.[23] Additionally, MIMOS Berhad, an agency under the Ministry of International Trade and Industry, in collaboration with tech giant Microsoft, launched the Centre of AI for Future Industry in March 2019,[24] which is essentially a platform to facilitate the adoption of AI innovations for local industry players. Ergo, it is undeniable that AI has sought prominence in the technological landscape in Malaysia in recent years, as seen in the increasing deployment of AI solutions across various sectors such as the legal services,[25] healthcare[26] and banking[27] sectors, to name a few.

Despite the apparent appetite for AI, the current legislative environment in Malaysia remains unequipped to regulate the ever-evolving complexities of AI and the concerns that come along with it.

For example, the Personal Data Protection Act 2010 (**PDPA**) regulates the processing of personal data of individuals in respect of commercial transactions[28] and applies to any person who processes and has control over or authorises the processing of personal data (i.e. data users). Data users are required to comply with the seven personal data protection principles in processing personal data, which include:

(a) the General Principle: Data users must obtain consent of data subjects before collecting their personal data;[29]

(b) the Notice and Choice Principle: Data users must inform data subjects, by way of a written notice, regarding the use of their personal data;[30]

(c) the Disclosure Principle: Data users must not, without the consent of data subjects, disclose personal data for any purpose, other than for purposes for which they were collected;[31] and

(d) the Security Principle: Data users must take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.[32]

An obvious limitation of the PDPA vis-à-vis AI is that it is only applicable to personal data processed in commercial transactions. Therefore, it is arguable that the AI-based processing of personal data for non-commercial purposes, such as security and monitoring or research and development, would be outside of the scope of the PDPA, thereby taking away the protections afforded to data subjects under the PDPA. Additionally, the PDPA does not impose direct obligations on data processors[33] in processing personal data on behalf of a data user, which could raise concerns in the event that data processors engage in AI-based processing. Further, the PDPA does not have extraterritorial affect which would mean that use of AI in processing personal data of data subjects in Malaysia that takes place outside of Malaysia that is not intended to be further processed in Malaysia will not be subject to the PDPA.[34] The PDPA also lacks the requirement to notify both the data subject and the relevant authority in the event of a data breach, which has proven to be a grave concern when it comes to AI.[35] As it stands, the PDPA is notably not up to par with international standards of personal data protection and privacy laws.[36]

---

23 As published on the MDEC website, available at https://mdec.my/about-malaysia/government-policies/

24 Available at http://www.mimos.my/services/national-facilities/centre-of-artificial-intelligence-for-future-industry-caifi/

25 "Introducing ASKAILA, Malaysia's first artificial legal assistant: An AI That Specializes in Labor Law", *Malaysiakini* (11 December 2020) https://www.malaysiakini.com/announcement/554776

26 "Skymind Helps Boost Malaysian Hospitals AI Healthcare Capabilities", *Business Today* (15 April 2020) https://www.businesstoday.com.my/2020/04/15/skymind-helps-boost-malaysian-hospitals-ai-healthcare-capabilities/

27 "RHB Bank Launches Malaysia's First AI-Powered SME Financing Mobile App, Aims to Finance RM500m", *The Edge* (3 August 2020) https://www.theedgemarkets.com/article/rhb-bank-launches-malaysias-first-aipowered-sme-financing-mobile-app-aims-finance-rm500m

28 Preamble to the PDPA

29 PDPA, s 5

30 PDPA, s 7

31 PDPA, s 8

32 PDPA, s 9

33 "Data processors" are defined under s4 of the PDPA as any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.

34 PDPA, s 3(2)

35 "Amazon Does the Unthinkable and Sends Alexa Recordings to the Wrong Person", *Forbes* (20 December 2018) https://www.forbes.com/sites/kevinmurnane/2018/12/20/amazon-does-the-unthinkable-and-sends-alexa-recordings-to-the-wrong-person/?sh=4ed9f53ca5df

36 Note that the Personal Data Protection Commissioner issued a Public Consultation Paper on the Review of the PDPA in February 2020 for public consultation, with the objective of enhancing the existing provisions under the PDPA to be parallel with international standards. Following the end of the consultation period in March 2020, the Commissioner has yet to publish any potential steps or measures to be taken in effecting the proposed amendments to the PDPA.

Exciting times ahead

The Proposed Regulation may be the first comprehensive regulatory framework to regulate AI, but other countries have not fallen short in their approaches to monitor the deployment of AI. The US Federal Trade Commission recently published guidance for companies on the use of AI in ensuring truth, fairness and equity[37] in addition to its recommendations on using AI and algorithms.[38] The Office of the Privacy Commissioner of Canada published its recommendations for a regulatory framework for AI and reforms to its data privacy laws in November 2020.[39] Closer to home, the Personal Data Protection Commission of Singapore has released two editions of a Model AI Governance Framework for public consultation, which provides guidance to private sector organisations in addressing key ethical and governance issues when deploying AI solutions.[40]

From the local perspective, the Malaysia Digital Economy Blueprint was published in March 2021 by the Prime Minister's Department which, among others, includes several initiatives relevant to AI. These include to increase adoption of digital technologies such as AI to enable the transformation of government operating models[41] and to upskill the workforce's digital skills in AI.[42] Additionally, one of the strategies set out in the blueprint is the streamlining of regulatory requirements to respond to the digital economy which includes strengthening the intellectual property regulatory framework and enforcement,[43] implementing competition policies to achieve a level playing field in the digital economy[44] and a review of existing laws on personal data protection and cyber security.[45]

It will undoubtedly be interesting to see the impact that the enforcement of the Proposed Regulation will have on AI players globally as well as on the regulation of AI in other jurisdictions. On the domestic front, the government policies and strategies described above clearly exhibit our eagerness in embracing AI, although it remains to be seen how this will translate into the development of a regulatory framework capable of ensuring the use and supply of AI that is secure, ethical and business-friendly.

LH-AG

About the author

Eleena Abd Wahab (eaw@lh-ag.com) is a senior associate with the Technology, Media and Telecommunications Practice and is part of a team headed by Teo Wai Sum.

Teo Wai Sum
Partner (Corporate Advisory)
Technology, Media & Telecommunications
E: tws@lh-ag.com

37 "Aiming for Truth, Fairness, and Equity in Your Company's Use of AI", Federal Trade Commission (19 April 2021) https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai

38 "Using Artificial Intelligence and Algorithms", US Federal Trade Commission (8 April 2020) https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms

39 "A Regulatory Framework for AI: Recommendations for PIPEDA Reform", Office of the Privacy Commissioner of Canada (November 2020) https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/

40 "Singapore's Approach to AI Governance", Personal Data Protection Commission Singapore https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework

41 Malaysian Digital Economy Blueprint, p 46 https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf

42 *Ibid*, p 66

43 *Ibid*, p 53

44 *Ibid*, p 54

45 *Ibid*, p 74