



DREWACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

EVERYTHING YOU
NEED TO KNOW
ABOUT AI AND ITS
REGULATION IN
15 MINUTES

LEGAL
GUIDES
2023

CONTENTS

- **An introduction to AI, and a framework to understand it**
- **Part 1: What is AI and what are its features that would affect the way existing laws are applied**
- **Part 2: Singapore's developments on AI**
- **Part 3: International developments on AI**
- **Part 4: A framework for navigating the use of AI in light of local and international developments**
- **Conclusion**

**EVERYTHING YOU NEED TO KNOW
ABOUT AI AND ITS REGULATION
IN 15 MINUTES**

An introduction to AI, and a framework to understand it

“Artificial intelligence”, or “AI”, is a topic that is increasingly relevant these days, from the use of ChatGPT to generate content, to algorithms used to execute financial trades, to autonomous vehicles plying the roads. AI can process information at a speed far greater than any human, so it is a convenient “tool”, where instead of a human making decisions, analysing information, or generating content, it is now done by algorithms that have been trained on data. It is thus important to know what artificial intelligence is and what it can and cannot do, in order to meaningfully discuss whether we should regulate its use and how.

In our view, it is helpful to break down the AI landscape into 4 parts, and we will use this framework to analyse all issues arising from the use of AI:

- (a) **What is AI?** This is a technical discussion of what artificial intelligence is, so that we can understand what are its features that may affect the way existing laws are applied, such as conventional principles of liability.
- (b) **What should AI be?** This is a discussion of the principles that govern the use of AI, with the intention of making the use of AI as safe as possible. The principles are that AI must be “explainable”, “transparent” and “fair”, and extend into data governance, personal data protection and cybersecurity measures. Countries around the world have set out their own guidance frameworks, from Singapore’s Model Artificial Governance Framework (“Model Framework”), to the European Union’s Artificial Intelligence Act (“EU AI Act”). There is emerging global consensus on how the use of AI should be governed, centering on “accountability” on the part of persons deploying AI, and “awareness” (that they are subject to such decisions, and how AI works) on the part of persons who are subject to decisions made by AI.
- (c) **Testing: how do you know (the use of) AI is what it claims to be?** To ensure that guidelines or legislation on AI governance are effective, there must be a means to measure compliance with them. Singapore has developed self-assessment guides for organisations, as well as “AI Verify”, a series of process and technical checks. The EU also has introduced the concept of “conformity assessments” which assess how the AI system complies with the requirements in the EU AI Act before it is placed on the market.
- (d) **What happens when things go wrong?** Despite the measures put in place to ensure the use of AI is as safe as possible, there will be situations where the use of AI results in harm to a person, as risks can be reduced but not eliminated entirely. The EU offers a helpful categorisation of the risks as (traditional) “safety risks” (e.g. death, injury or property damage) or “fundamental rights risks” (e.g. discrimination, manipulation, loss of privacy).¹ In such a case, how will existing negligence law, product liability law, contract law, and other legal principles operate to give the injured party a remedy, and will their application be affected by the unique features of AI?

To address these key questions, and give an overview of how the present state of regulation of the use of AI will impact you, this introductory article to our series on AI will cover 4 key issues. We have also integrated further reading links to articles we have written on selected topics for you to find out more.

- (a) Part 1: What is AI and what are its features that may affect the way existing laws are applied?
- (b) Part 2: Singapore’s developments on AI (regulatory and non-regulatory)
- (c) Part 3: International developments on AI (regulatory-only) and their significance to Singapore

¹ See the Explanatory Memorandum to the European Commission’s Proposal for a Directive of the European Parliament and of the Council on adopting non-contractual civil liability rules to artificial intelligence (October 2022), available at: https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf.

- (d) Part 4: The framework for navigating the use of AI in light of local and international developments, namely (i) what principles the use of AI should adhere to; (ii) how do we know those principles are being followed (*testing/audits*); and (iii) what happens if AI does not perform as expected (*liability*).

Part 1: What is AI and what are its features that would affect the way existing laws are applied

AI is broadly defined as “a set of technologies that seek to simulate human traits such as knowledge, reasoning, problem solving, perception, learning and planning, and, depending on the AI model, produce an output or decision (such as a prediction, recommendation and/or classification)”.²

For clarity, these are the definitions of the terminology we will use³:

- (a) “Algorithms” are a set of rules/instructions like mathematical formulas and programming commands given to a computer for it to do a task;⁴
- (b) An “AI model” is created when algorithms analyse data, leading to an output/result which is examined and the algorithms iterated, until the most appropriate model emerges⁵- it is akin to what has been “learnt” by the algorithms (in the sense of them having been adjusted/calibrated) after they have analysed all the training data;
- (c) An “AI system” is the model that is selected and deployed, such as by being incorporated into an application⁶.

The most prevalent form of AI is “machine learning”, where statistical techniques are applied to identify patterns in large amounts of data.⁷ Unlike rule-based decisions, where a human must conceive the rules so there are predetermined responses to a set of conditions, with machine learning, the machine learning system is set up to “learn” its own responses to conditions under a training regime, and will get better with time (think of a learner driver getting better with practice).⁸ There are 2 main approaches to machine learning:

- (a) Supervised learning – which is good for classifications (e.g. is this email spam) or making predictions (e.g. predicting the price of a house). A labelled dataset will be used to train the machine so the algorithm knows what the expected output is. This is the more commonly used approach.
- (b) Unsupervised learning – which is good for grouping things with similar traits together, and looking for relationships between data (e.g. customers who bought X also bought Y). It can discover patterns without the need for human intervention, and uses unlabelled datasets.

Because of the way machine learning works, it is often called a “black box”, where even the humans who designed the model cannot understand how the variables are combined or jointly related to each other to make a prediction.⁹

² Singapore’s Model Artificial Intelligence Governance Framework (Second Edition) (“**Model Framework**”) at [2.15].

³ These 3 terms are used but are not defined in the Model Framework, but their meaning can be inferred from the context in which they are used.

⁴ As defined in the Singapore Academy of Law, Law Reform Committee’s report on “Applying Ethical Principles for Artificial Intelligence in Regulatory Reform” (July 2020), available at: https://www.sal.org.sg/sites/default/files/SAL-LawReform-Pdf/2020-09/2020%20Applying%20Ethical%20Principles%20for%20AI%20in%20Regulatory%20Reform_ebook.pdf

⁵ See [3.20] and [3.21] of the Model Framework.

⁶ See [3.21] of the Model Framework.

⁷ *The Law of Artificial Intelligence*, Matt Hervey and Matthew Lavy (“*TLIA*”) at page 1.

⁸ *TLIA* at page 9.

⁹ See article “Why Are We Using Black Box Models in AI When We Don’t Need To? A Lesson From an Explainable AI Competition” by Cynthia Rudin and Joanna Radin (published 22 Nov 2019), Issue 1.2, Fall 2019 Harvard Data Science Review, available at: <https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/8>.

Yet, just because a machine makes a recommendation or decision does not fundamentally change things. We still have the same considerations as if the decision is to be made by a human, in that the data relied on must be accurate, the decision must be correct and fair, and people affected must have means to appeal against the decision.

Because of the way AI works, we are of the view that there are 3 unique features of AI which will require us to evaluate whether our existing legal principles (common law and legislation) can deal with the use of AI to effectively allocate risk between all involved persons. The 3 features are:

- (a) **AI is a “black box” (which affects how we can explain its workings)** – we don’t always know how or why it arrived at a particular result especially with machine learning, where the machine learns its own rules and uncovers hidden relationships in the data beyond what unaided human observation can do.¹⁰ Rule-based systems, in contrast, are easier to explain because of their if-then structure. “Explainable AI” is thus a growing field of research in machine learning so as to reduce its opacity by explaining how AI functions and how it arrives at a particular decision. There are also strong policy reasons not to allow persons (e.g. the developers of the AI) to escape liability on the basis that the result cannot be explained, because at the end of the day it must always stem from some form of programming by a human — a machine “can only interpret what has been taught (i.e. programmed)”¹¹.
- (b) **AI is self-learning/autonomous** – with machine learning, the AI model has the ability to automatically learn and improve from experience without being explicitly programmed, which means that its behaviour may not be fully foreseeable in all situations even if you know what is the algorithm that directs the learning.¹² This is further compounded in cases of AI systems that have continuous learning capabilities, which means they continue to learn even after they are deployed, and can change their behaviour in response to real-world data input into them.¹³ They are in contrast to AI systems that are ‘fixed’ once deployed, akin to a person’s knowledge being frozen at a certain point in time.
- (c) **Many persons involved in its development** instead of a clearly identifiable person – from selecting the datasets, to training the AI, to designing the algorithm, monitoring the output, etc. – who should be held responsible in the event the AI output is not as expected? The person (procurer) who requires another person to develop an AI system for them could also have a role in constructing the AI system by selecting and inputting the relevant data into the system (and the procurer might even feed in erroneous or insufficient data), in contrast to ordinary computer systems that are immediately ready for use by the procurer who is not involved in its construction.¹⁴

Part 2: Singapore’s developments on AI

Singapore’s regulations and initiatives in relation to AI

There is no legislation in Singapore governing the general use of AI, in contrast to EU’s Artificial Intelligence Act or the USA’s Algorithmic Accountability Act. However, Singapore has legislation for autonomous vehicles, in line with countries all around the world, because our road traffic laws are premised on having a human driver. For more information on autonomous vehicles, please refer to our

¹⁰ *TLIA* at page 28.

¹¹ See paragraph 1.13 of the Singapore Academy of Law Law Reform Committee Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars (September 2020).

¹² *TLIA* at page 121.

¹³ See [3.33] of the Model Framework; section 9.2 of HSA’s Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach (April 2022); preamble (66) of the EU AI Act; and “The Next-Generation AI Brain: How AI Is Becoming More Human” by Max Versace, available at: <https://www.forbes.com/sites/forbestechcouncil/2018/04/09/the-next-generation-ai-brain-how-ai-is-becoming-more-human/?sh=26340475733b>.

¹⁴ See “B2B Artificial Intelligence Transactions: A Framework for Assessing Commercial Liability” by Ernest Lim, ([2022] SJLS 46-74) at 47.

article “*Autonomous Vehicles in Singapore*”¹⁵. In all cases, it is important to note that regulation would be of the use of AI, and not AI itself. It is not feasible to regulate the technology alone without reference to its use.

Singapore announced our National AI strategy¹⁶ in 2019, outlining Singapore’s aim of becoming a leader in developing and deploying scalable, impactful AI solutions across key sectors of high social and economic impact by 2030. The 5 key sectors Singapore is presently focussing on are (a) transport and logistics, (b) municipal services, (c) education, (d) healthcare and (e) border clearance/border security.

In the same year, the Infocomm Media Development Authority (“**IMDA**”)/Personal Data Protection Commission (“**PDPC**”) also released the Model Artificial Intelligence Governance Framework (“**Model Framework**”) – it is Asia’s first model AI governance framework. It is not a legally binding text but organisations are urged to comply with it. For details of how organisations may implement the Model Framework, please refer to the [explainer](#)¹⁷ which we have written. The Model Framework is to be read in tandem with the Implementation and Self-Assessment Guide for Organisations (“**ISAGO**”), which adopts a risk-based approach when determining the level of safeguards for AI, and comprises a series of questions for organisations to run through to assess their compliance with the principles in the Model Framework. A further voluntary self-assessment framework with both technical tests and process checks (called “AI Verify”) is being trialled as at May 2022 — it does not define ethical standards but allows AI developers to validate their claims about their AI systems against internationally accepted principles.¹⁸

Regulators in other sectors have also issued guidance, for example:

- (a) the Intellectual Property Office of Singapore has released the *IP and Artificial Intelligence Information Note* to provide an overview of how different types of IP rights can be used to protect AI inventions¹⁹;
- (b) for the financial sector, the Monetary Authority of Singapore has released the Fairness, Ethics, Accountability and Transparency (FEAT) principles²⁰, and embarked on the Veritas initiative to help the financial industry implement the FEAT principles²¹;
- (c) the healthcare regulators have released the *Artificial Intelligence in Healthcare Guidelines (AIHGLE)* in October 2021 to complement the existing regulatory requirements for AI-enabled medical devices.²²

The Government has further affirmed its commitment to developing AI in Singapore by investing \$71 million to develop the workforce’s expertise in AI, and open 3 new centres of innovation for organisations to test their AI ideas²³. There is also an “AI for everyone” (AI4E) course developed by AI Singapore (a partnership between government agencies and academia) that is rolled out to workplaces and educational institutions.

¹⁵ Please see our article on “Autonomous Vehicles in Singapore”, available at:

<https://www.drewnapier.com/DrewNapier/media/DrewNapier/Autonomous-vehicles-in-Singapore-laws-and-liability.pdf>.

¹⁶ See document “National Artificial Intelligence” by Smart Nation & Digital Government Office (published Nov-2019), [Smart Nation Singapore, available at: <https://www.smartnation.gov.sg/files/publications/national-ai-strategy.pdf>

¹⁷ Please see our article on “Issues you must consider before deploying artificial intelligence in your business: an explainer of Singapore’s Model Artificial Intelligence Governance Framework”, available at:

<https://www.drewnapier.com/DrewNapier/media/DrewNapier/Incorporating-Singapore-Model-Artificial-Intelligence-Governance-Framework-into-your-business.pdf>

¹⁸ <https://www.weforum.org/agenda/2023/01/how-singapore-is-demonstrating-trustworthy-ai-davos2023/>

¹⁹ <https://www.ipos.gov.sg/docs/default-source/default-document-library/ip-and-ai-info-note.pdf>

²⁰

<https://www.mas.gov.sg/-/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf>

²¹ <https://www.mas.gov.sg/schemes-and-initiatives/veritas>

²² [https://www.moh.gov.sg/docs/librariesprovider5/eguides/1-0-artificial-in-healthcare-guidelines-\(aihgle\)_publishedoct21.pdf](https://www.moh.gov.sg/docs/librariesprovider5/eguides/1-0-artificial-in-healthcare-guidelines-(aihgle)_publishedoct21.pdf)

²³ <https://www.enterprisesg.gov.sg/resources/media-centre/news/2022/october/singapore-to-invest--71m-to-attract--develop-ai-tech-talent>

Nevertheless, there are some limits to Singapore’s use of AI at present – such as the use in sentencing. At the Sentencing Conference in October 2022, the Chief Justice said that Singapore would not be using AI to generate sentencing recommendations or assess an offender’s risk of recidivism, as this could prejudice certain groups of persons, and the underlying algorithms and data are opaque. Instead, Singapore’s approach will be to set up a sentencing advisory panel, where sentencing guidelines that are persuasive but not binding on the courts will be issued and made accessible to the public online.²⁴

Does it matter that there’s no legislation governing the use of AI in Singapore (aside from autonomous vehicles)?

At present, there is a light-touch approach to the regulation of use of AI in Singapore, in the form of guidance notes and voluntary guidelines, and we are of the view this is appropriate given that the technology changes very quickly. Guidelines are agile and suitable for an area where change is rapid, unlike an Act of Parliament which must follow certain procedural rules for introduction or amendment. Also, legislation need not always be the first port of call – public education and codes of practice can also shape behaviour, and the common law is also flexible and can respond to an evolving legal landscape.

Furthermore, whether or not there is legislation, the fact that guidelines are published and public/industry consultations are conducted shows that the government, the private sector and the general public are looking at AI seriously, and the resulting documents reflect the principles that are important to them. Unlike legislation, guidelines do not have sanctions for non-compliance, but they do set out good practice, and following them can build trust in an organisation’s use of AI.

Nevertheless, Singapore does not intend to go at it alone, and international developments will play a role in shaping our regulation of the use of AI. Singapore announced in our 2019 National AI Strategy that Singapore intends to actively participate in standard setting with key international organisations such as the World Economic Forum, the Organisation for Economic Co-operation and Development and the International Organization for Standardization.

Part 3: International developments on AI

How are AI developments around the world significant to Singapore?

Developments around the world show increased public and private sector scrutiny of AI. In recent years, at least 70 countries have developed a national AI strategy,²⁵ and there are ongoing public consultations, discussions in international fora, and an increase in the pace of legislation and guidelines being introduced over the past few months.²⁶ The international discourse has also shifted away from legal personality for AI.

At present, there is no legislation regulating the general use of AI yet around the world²⁷ – the most prominent of such legislation, mooted in the EU (Artificial Intelligence Act) and USA (Algorithmic Accountability Act), have yet to pass into law and come into force, so the next 1 to 2 years will be very keenly watched! However, there is legislation concerning the use of AI in specific sectors, such as using automated employment decision tools in New York (where the tool must be subject to a bias audit)²⁸, China’s regulations governing companies’ use of algorithms in online recommendation systems²⁹, and

²⁴ <https://www.straitstimes.com/singapore/courts-crime/s-pore-not-likely-to-use-ai-in-sentencing-in-foreseeable-future-chief-justice>

²⁵ Based on a review of the OECD’s live repository of AI strategies and policies from 69 countries, territories and the EU at <https://oecd.ai/en/dashboards/overview> (as at 26 April 2023).

²⁶ Based on our monitoring of reports on AI on news aggregator sites.

²⁷ Based on a review of the OECD’s live repository of AI strategies and policies from 69 countries, territories and the EU at <https://oecd.ai/en/dashboards/overview> (as at 26 April 2023), as well as a monitoring of news reports and articles.

²⁸ <https://news.bloomberglaw.com/daily-labor-report/new-york-city-ai-bias-law-charts-new-territory-for-employers>

²⁹ http://english.www.gov.cn/news/topnews/202201/04/content_WS61d3f8fbc6d09c94e48a31d1.html; see also <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/>

using autonomous vehicles (all around the world) since road transport legislation is (previously) premised on there being a human driver.

Significant developments in some key jurisdictions (EU, USA, UK, China, Japan, Australia) will be spotlighted, followed by an analysis of these developments. The jurisdictions will generally be split into those who think legislation to regulate the use of AI is necessary (EU and USA, where both propose to regulate high-risk uses of AI), and those who are adopting a wait-and-see approach by issuing guidelines for the industry first (UK, Japan, Australia, Singapore). We have placed China in its own category as well as its model is *sui generis* compared to the other jurisdictions.

It is important to pay attention to these international developments because technology knows no boundaries. If you wish to export your technology to another country, you would have to comply with their laws in place. The EU AI Act will also apply to providers (developers of AI systems) and users (any person using an AI system under its authority) of AI systems that are established outside the EU, so long as the output produced by those systems is used in the EU.³⁰

We also envision that there will be growing international harmonisation of laws governing AI so that AI technology can be exported. To this end, the International Organization for Standardization has been setting standards – it recently released (in February 2023) guidance for organisations that develop or use products, systems and services that utilise AI on how they can manage risk specifically related to AI, and has also introduced standards for autonomous vehicle testing. The first international AI Convention is also in the works, with the Council of Europe Committee on Artificial Intelligence releasing to the public a ‘zero draft’ of the convention in February 2023. This convention aims to ensure that the development of AI systems respects human rights, democracy and the rule of law, and will be open to participation by non-EU member states.³¹

European Union

There are 3 key legislative proposals arising from the EU — the EU Artificial Intelligence Act (which generally focuses on safety of AI) the AI Liability Directive³² and the Revised Product Liability Directive³³(which generally focus on liability arising from the use of AI). All are not yet in force.

The AI Act was introduced by the European Commission in 2021 to set out a legal framework for trustworthy AI, and to prevent regulatory fragmentation where each member state sets out its own principles as opposed to a harmonised approach. Trilogue discussions between the European Commission, European Council and European Parliament are expected to be completed by end-2023, and the text of the Act may be subject to further changes. The AI Act also adopts a risk-based approach, with 3 categories: some uses of AI are prohibited³⁴, high-risk³⁵ uses of AI subject to regulation, and all other (low-risk) uses of AI subject to voluntary codes of conduct.

A high-risk AI system must comply with the requirements in the AI Act, covering everything from having a risk management system to the quality of data sets used, technical documentation and record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity. The high-risk AI system is subject to a conformity assessment (to assess its compliance with the requirements in the AI Act) before it is put on the market:

³⁰ See preamble (11) of the EU AI Act, and Article 2 of the EU AI Act.

³¹ <https://www.dataguidance.com/news/international-coe-committee-publishes-revised-zero>

³² This is the proposal for a Directive on adopting non-contractual civil liability rules to artificial intelligence, published on 28 September 2022 and available at https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf

³³ This is the proposal for a Directive on liability for defective products, published on 28 September 2022 and available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495>

³⁴ Such as those which deploy subliminal techniques to influence a person’s behaviour, or any form of “social-scoring” systems (see Article 5).

³⁵ Where the AI system is intended to be used as a safety component of a product or is itself a product, or if the AI system is of a type referred to in Annex III of the Act, where it is used in areas such as biometric identification, education, employment and law enforcement.

- (a) Where the AI system is to be used as a safety component of products (such as machinery, lifts, toys), or is itself the product, this assessment must be done by a third party (and other existing sectorial safety legislation will apply);
- (b) Where the AI system is a stand-alone one (as set out in Annex III, where it is used in areas such as law enforcement, determining access to educational institutions or employment, determining access to essential public and private services, or migration, asylum and border control management), the conformity assessment can be a self-assessment (unless it is for the remote biometric identification of persons), and the AI system must also be registered on an EU database.

There will also be a requirement for post-market monitoring and reporting, such that serious incidents and malfunctions must be reported to the public authorities.

Where risk materialises despite all the measures to ensure the safety of the use of AI and minimise its risks, the law must also address this. The EU has thus recently (in September 2022) put forth 2 new liability rules for AI systems that will make it easier for plaintiffs to bring a case – but they will be operational in 2024 or 2025 at the earliest. The EU AI Liability Directive introduces a rebuttable presumption of causality between the defendant’s fault and resulting damage arising from the AI system’s output (or failure to produce output), and also allows the court to order disclosure of relevant evidence to assist the claimant in bringing its case. For the Revised Product Liability Directive, it introduces new provisions to address liability for products such as software (including AI systems).

USA

One of the key developments in the USA is the Algorithmic Accountability Act of 2022, introduced in February 2022. The USA has also released other guidance material³⁶, but we will focus on the Algorithmic Accountability Act for the purposes of contrasting it with EU’s Act.

The Algorithmic Accountability Act is presently in Committee – it has not yet passed. The Act will allow the Federal Trade Commission to require entities to conduct impact assessments of their automated decision systems, evaluating and documenting everything from their protection of private data, testing the performance of the automated system, and training employees on using the system. If entities are unable to comply with any of the requirements, the reason for not being able to comply must be documented. Entities then report the results to the Commission in the form of a “summary report”, and the Commission will, on a yearly basis, publish publicly on their website a report summarising the information in all the “summary reports” received by it, so that the public may access the information.

Similar to the EU, the US Act applies to high-risk decisions, framing it as a “critical decision” that has a material/significant impact on a person’s life, such as in areas of healthcare, employment and immigration. However, there are also differences between the EU and US way of regulation, such as:

- (a) The US Act focuses on disclosure of how an entity measures up against the reporting requirements in the Act, which will be publicised. In contrast, the EU Act requires the AI system to comply with a set of requirements before it can be put on the market.
- (b) The US Act is only applicable to entities above a certain size (measured in terms of finances or the number of persons whose data it uses), while the EU Act does not make such distinction.

China

China has not introduced nationwide legislation regulating the use of AI generally akin to that in the EU and US (which are still at a proposal stage), but it has promulgated municipal legislation on the same, with concepts of ‘high risk’, ‘medium risk’ and ‘low risk’ uses of artificial intelligence, which will be

³⁶ E.g. the Blueprint for an AI Bill of Rights (October 2022), and most recently in January 2023, an “Artificial Intelligence Risk Management Framework” by the National Institute of Standards and Technology.

regulated differently (as set out in its Regulations for the Promotion of the Artificial Intelligence Industry in Shenzhen Special Economic Zone, which is already in force).³⁷ Additionally, China has enacted legislation on targeted fronts, such as on the use of algorithms on online recommendation systems (e.g. not to use personal data to offer different prices to consumers, not to push content such as alcohol and tobacco to minors), and also on the use of deepfakes and other generative AI³⁸. China has also articulated governance principles (which are largely similar to Singapore's)³⁹.

UK, Australia, Japan

The UK, Australia and Japan very similar to Singapore and have yet to propose legislation that regulates the use of AI in general. Instead, each of the jurisdictions has issued guides for the industry, similar to Singapore's Model AI Framework, with the more significant ones as follows:

- (a) UK – ICO's Guidance on the AI Auditing framework⁴⁰; ICO Guidance on AI and data protection⁴¹; Establishing a pro-innovation approach to regulating AI (18 July 2022)⁴²;
- (b) Australia – AI Ethics Framework (2019)⁴³;
- (c) Japan – Government Guidance for Implementation of AI Principles ver. 1.1 (28 January 2022)⁴⁴.

In particular, the UK regulators⁴⁵ have stated that they are keen to have non-legislative solutions first like guidelines. The UK does not see a need for regulation at this stage but will not rule it out if this is what regulators need to implement the framework. But even so, legislation would be the exception, and it would be for AI uses with high-impact risk on people. Sector-specific legislation is also preferred.

Part 4: A framework for navigating the use of AI in light of local and international developments

We recommend that the global developments in AI be assessed in 3 parts:

- (a) **what AI should be** (i.e. what principles the use of AI should adhere to);
- (b) **how do we know whether AI is as it should be** (how do we know those principles are being followed, which requires the use of testing frameworks/audits);
- (c) **what happens when AI does not perform as expected** (even if it complies with requirements in (a) and passed the test in (b)) (liability).

(1) What AI should be

The first is that principles on what AI should be are converging – we have distilled 5 common principles from our study of different key jurisdictions:

- (a) AI systems should be explainable;

³⁷ Translation available at: https://cset.georgetown.edu/wp-content/uploads/t0480_Shenzhen_AI_regs_EN.pdf - see in particular Article 66.

³⁸ <https://arstechnica.com/information-technology/2022/12/china-bans-ai-generated-media-without-watermarks/> and <https://www.holisticai.com/blog/china-ai-regulation>

³⁹ <https://www.loc.gov/item/global-legal-monitor/2019-09-09/china-ai-governance-principles-released/>

⁴⁰ <https://ico.org.uk/media/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf>

⁴¹ <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/>

⁴² <https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement>

⁴³ <https://www.industry.gov.au/science-technology-and-innovation/technology/artificial-intelligence>

⁴⁴ https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20220128_2.pdf

⁴⁵ <https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement> (18 July 2022).

- (b) AI systems should be fair: endeavour to minimise bias/discrimination from development to deployment;
- (c) AI systems should be transparent: disclose of the use of AI (including how it reaches a decision) to the affected person;
- (d) Providing for an appeal/review of decision made by AI where appropriate;
- (e) Different safeguards are needed depending on the “risk” or severity of impact on human – not all uses of AI must be regulated, where low-risk uses can have voluntary guidelines.

The principles can be summed up as: “accountability” on the part of the person deploying the AI, and “awareness” on the part of the person who is the subject of the AI decision.

(2) How do we know whether AI is as it should be (testing frameworks/audits)

The second is then what action is to be taken to turn this ideal state into a reality, with safeguards on the way AI is used and developed – some countries are of the view legislation is required for high-risk uses (e.g. EU, US), while others are of the view that guidelines are sufficient for now, taking a wait-and-see approach (Singapore, Japan, Australia, UK). China has its own unique model as well.

In our view, if AI is to be *X, Y and Z* and if there are consequences for not doing so, then there must be a way to determine whether it is in fact *X, Y and Z*, whether by self-assessment or by third party assessment. This is where testing comes in. Legislation would be a reality once testing mechanisms are settled (otherwise it cannot be enforced), and when sufficient use cases have been analysed to chart the regulatory approach so as not to over-regulate.

On the testing front, this is a developing area around the world that is coming into the spotlight, now that countries have a clearer sense of what they want AI to be. There would be 2 main types of tests – (a) the use of technical tools/programs to test an algorithm’s outputs or inspect how it works, and (b) a more normative assessment where a series of questions is asked and processes assessed (including checking documentation) in response to those questions. There is also the question of who will carry out the audit – regulators or accredited third-party auditors or self-audits – this area is still developing, because until common standards for audits are agreed on, audits will vary (areas audited, quality of auditor).⁴⁶

In Singapore, we have the ISAGO for organisations, a series of questions they can run through to self-assess their compliance with the Model Governance Framework. In May 2022, Singapore launched A.I. Verify, an AI Governance Testing Framework and Toolkit for AI system owners and developers who wish to verify their AI systems against 8 internationally accepted ethics principles. It has both technical tests and process checks, and does not define standards (e.g. no pass/fail) — organisations can just use it to see how they measure up to those principles. It is presently in its pilot testing stage.

Outside of Singapore, the US Algorithmic Accountability Act of 2022 requires organisations to self-report on their compliance with a list of requirements set out in the Act, and the EU AI Act requires high-risk AI systems to pass a conformity assessment before they are placed on the market, where depending on the nature of the system, the assessment can be carried out by the entity itself, or must be by a third-party.

(3) What happens when AI does not perform as expected?

“Safety and liability are two sides of the same coin”⁴⁷. The principles governing the use of AI (e.g. explainability, transparency, data governance, monitoring, cybersecurity, human oversight, etc.) can

⁴⁶ <https://www.gov.uk/government/publications/findings-from-the-drcf-algorithmic-processing-workstream-spring-2022/auditing-algorithms-the-existing-landscape-role-of-regulators-and-future-outlook>

⁴⁷ See the Explanatory Memorandum to the EU AI Liability Directive.

reduce the risks for safety and protect fundamental rights, but they cannot eliminate risk entirely. There is still the chance that harm will be caused to persons (whether or not the governance principles are complied with), and this can take the form of:

- (a) Fundamental rights risks (e.g. discrimination, manipulation, loss of privacy); and
- (b) Safety risks (death, injury and property damage).

Therefore, the conversation about liability arising from the use of AI is also coming to the forefront internationally, with regulators having to tread a fine balance between encouraging innovation and ensuring public safety. Most recently (29 March 2023), the UK has announced that it is not taking a position on liability yet, and will be consulting with the industry first as it is a complex topic.⁴⁸ The EU has published the AI Liability Directive and Revised Product Liability Directive, but they do not fundamentally rewrite the rules of liability, and only make it easier for plaintiffs to bring a claim. Compliance with the AI governance principles (whether in guidelines or legislation) is unlikely to be a shield from liability should it arise, but it can go some way towards mitigation.

Conclusion

We hope that in reading the articles across this microsite, you will gain an understanding of what is AI, how its use is being regulated, and most importantly, how to think about it, so that you can develop an AI strategy to navigate the volume of regulations and guidelines being introduced around the world, and understand your (new) obligations under them.

The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances. Copyright in this publication is owned by Drew & Napier LLC. This publication may not be reproduced or transmitted in any form or by any means, in whole or in part, without prior written approval.

⁴⁸ <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper> at paragraphs 80 - 85.

DREW DATA PROTECTION & CYBERSECURITY ACADEMY

Drew Data Protection & Cybersecurity Academy (Drew Academy) was established in 2020 by Drew & Napier to help our clients build their capabilities and develop and implement organisational strategies, structures, policies and processes to meet their legal, regulatory and compliance obligations. Drew Academy offers a range of courses in areas such as data protection, cybersecurity, data governance and in-house commercial practice. A particular focus for us is the delivery of workplace learning solutions and development of customised training courses. We also offer outsourced DPO services and data protection consulting services through our experienced team of practitioners.

Drew Academy is helmed by Lim Chong Kin and David N. Alfred. Our course leaders are experienced in various aspects of data and cyber governance, data protection, cybersecurity engineering and in-house commercial practice.

ARTIFICIAL INTELLIGENCE AND DIGITAL TRUST

Drew & Napier's Artificial Intelligence (AI) and Digital Trust practice brings together its expertise across several technology-related domains and in fields as diverse as data protection, cybersecurity, healthcare, Fintech, intellectual property and competition law (to name a few) to advise clients on the full range of legal issues relating to AI and Digital Trust. In addition to advising on commercial, regulatory and international / cross-border issues, our advice extends into areas such as governance and ethics as we seek to enable our clients to navigate areas where laws and legal principles are still emerging.

Working together with the Drew Academy, we provide solutions that reflect our deep understanding of underlying technologies, the risks and uncertainties involved and practical business considerations. Internationally, there is a growing consensus on AI governance.

For more information on our experience,
please contact:



Lim Chong Kin

Managing Director, Corporate & Finance;
Co-Head, Data Protection,
Privacy & Cybersecurity Practice;
Co-Head, Drew Data Protection &
Cybersecurity Academy

T: +65 6531 4110

E: chongkin.lim@drewnapier.com



David N. Alfred

Director, Corporate & Finance;
Co-Head, Data Protection,
Privacy & Cybersecurity Practice;
Co-Head and Programme Director,
Drew Data Protection &
Cybersecurity Academy

T: +65 6531 2342

E: david.alfred@drewnapier.com



Cheryl Seah

Director, Corporate & Finance

T: +65 6531 4167

E: cheryl.seah@drewnapier.com



DREW ACADEMY
DATA PROTECTION & CYBERSECURITY SERVICES

10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

www.drewnapier.com/Academy

T: +65 6531 4152

F: +65 6535 4864

E: academy@drewnapier.com

In association with

 **DREW & NAPIER**