COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

Singapore

ARTIFICIAL INTELLIGENCE

Contributor

Drew & Napier LLC

Lim Chong Kin

Managing Director | chongkin.lim@drewnapier.com

Anastasia Su-Anne Chen

Director | anastasia.chen@drewnapier.com

Cheryl Seah

Director | cheryl.seah@drewnapier.com

This country-specific Q&A provides an overview of artificial intelligence laws and regulations applicable in Singapore.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

SINGAPORE
ARTIFICIAL INTELLIGENCE

1. What are your countries legal definitions of “artificial intelligence”?

Singapore has defined “artificial intelligence” within the Model Artificial Intelligence Governance Framework (“**Model Framework**”), issued by the Infocomm Media Development Authority (“**IMDA**”) and the Personal Data Protection Commission (“**PDPC**”):

> *Artificial intelligence (or “AI”) refers to 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).*

This Model Framework is a voluntary document, setting out ethical and governance principles for the use of AI and translating them into practical recommendations for organisations to adopt. It applies across all sectors.

2. Has your country developed a national strategy for artificial intelligence?

In 2019, Singapore announced its National AI strategy, aiming to become a leader in developing and deploying scalable, impactful AI solutions in key sectors of high value and relevance to citizens and businesses by 2030. Singapore is embarking on an initial tranche of national AI projects in 5 areas with strong social and economic impact for Singapore – (1) intelligent freight planning; (2) seamless and efficient municipal services; (3) chronic disease prediction and management; (4) personalised learning for students through adaptive learning and assessment; (5) border clearance operations to strengthen border security while improving traveller experience.

As of June 2023, the Singapore government has invested about S$500 million in AI research and development over the last 5 years. [1]

Footnotes:

1. About S$500 million invested in AI innovation in last 5 years: Josephine Teo, Startups & Tech – THE BUSINESS TIMES

3. Has your country implemented rules or guidelines (including voluntary standards and ethical principles) on artificial intelligence? If so, please provide a brief overview of said rules or guidelines. If no rules on artificial intelligence are in force in your jurisdiction, please (i) provide a short overview of the existing laws that potentially could be applied to artificial intelligence and the use of artificial intelligence, (ii) briefly outline the main difficulties in interpreting such existing laws to suit the peculiarities of artificial intelligence, and (iii) summarize any draft laws, or legislative initiatives, on artificial intelligence.

Singapore does not have legislation that specifically addresses the use of artificial intelligence across a variety of sectors (cf. the EU Artificial Intelligence Act which focuses on high-risk uses of AI). The government is presently not looking to enact regulation for AI, but is focusing its efforts on promoting the responsible use of AI though mediums such as the Model Artificial Intelligence Governance Framework, and its AI testing framework and toolkit called “AI Verify”. [1] The government will continue to monitor the state of technology and how it is being used before deciding on a regulatory approach.

However, Singapore has enacted laws in relation to specific applications of AI technology. Our Road Traffic Act 1961 was amended in 2017 to provide for the trial and use of autonomous motor vehicles, as our road traffic laws were previously premised on there being a human driver (previous uses of AVs on the roads would be by way of exemptions from the Act). In relation to

medical devices that incorporate AI technology ("AI-MDs"), these must also be registered under the Health Products Act 2007, as all medical devices must be registered regardless of whether they incorporate AI technology. However, the Health Sciences Authority's Regulatory Guidelines for Software Medical Devices specifies the additional information that must be submitted when registering an AI-MD, for example, information about the data sets used for training and validation, a description of the AI model, reports to substantiate its performance claims, and the level of human intervention in the system.

Nevertheless, in all instances where artificial intelligence technology is applied, existing laws can still apply. For example, tort law and contract law can apply where the AI system does not perform as expected, and the Personal Data Protection Act 2012 applies where the AI system is used to process personal data. Companies that develop or utilise AI systems must also comply with existing corporate laws, employment laws and competition laws, to name a few.

Our regulators have also issued a series of guidelines to assist the industry with utilising this new technology, such as:

a. IMDA/PDPC issued (in January 2020) the 2nd Edition of the "Model Artificial Intelligence Governance Framework", setting out key principles organisations must take into account when developing and deploying AI.

The Model Framework is based on 2 high-level guiding principles to promote trust in the use of AI, where organisations using AI in decision-making should ensure that the decision-making process is explainable, transparent and fair, and that AI solutions should be human-centric with human well-being and safety at the forefront. It is complemented by the Implementation and Self-Assessment Guide for Organisations which sets out a series of questions for organisations to self-assess how their practices align with the Model Framework.

b. IMDA issued (in June 2023) a paper on "Generative AI: Implications for Trust and Governance", which identifies 6 risks of generative AI and 6 governance approaches to mitigate those risks;

c. The Monetary Authority of Singapore (MAS) released (in November 2018) the "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector", and leads the Veritas consortium within the financial industry to promote the responsible use of AI;

d. The Intellectual Property Office of Singapore (IPOS) issued the "IP and Artificial Intelligence Information Note" to provide an overview of how different types of IP rights can be used to protect AI inventions.

Footnotes:

1. https://www.cnbc.com/2023/06/19/singapore-is-not-looking-to-regulate-ai-just-yet-says-the-city-state.html and https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2023/4/mci-response-to-pq-on-regulatory-framework-for-artificial-intelligence-governance-in-singapore?category=Cyber+Security

4. Which rules apply to defective artificial intelligence systems, i.e. artificial intelligence systems that do not provide the safety that the public at large is entitled to expect?

Singapore has not enacted legislation that specifically deals with defective artificial intelligence systems. It would thus fall to be governed by the existing regime for that particular product – for example, in the case of AI-MDs regulated under the Health Products Act 2007, the Authority may suspend or cancel the registration of such AI-MD if it has reasonable grounds to believe that the safety of the AI-MD has changed so as to render it unsuitable to continue to be registered, or if it is in the public interest to do so (see section 37 of the Health Products Act 2007).

Ordinary principles of tort and contract will also apply. Please see S/N 5 below for further details.

5. Please describe any civil and criminal liability rules that may apply in case of damages caused by artificial intelligence systems.

Civil liability

Where damage is caused by the AI system, the affected person may seek a remedy in tort or contract (if there is a contract between the parties). However, AI technology has some unique features that may affect how conventional tort and contract principles of liability are applied:

a. AI is a "black box" – it is not always possible to explain how or why the AI system reached a particular outcome even if the factors the

system is programmed to take into account are known, and the type of model chosen affects how easily the system can be explained, as some models are more complex than others – this would increase the difficultly in proving that the damage was the result of a defect in the programming of the AI system, as opposed to some other cause;

b. AI is self-learning, where it can learn from the data it has been exposed to during its training and improve the results generated without being explicitly programmed, meaning that the output of the system will not always be foreseeable;
c. AI has multiple people involved in its development, from procuring and selecting the datasets, to training the algorithm, to monitoring the performance of the algorithm – so it will be a complex fact-finding exercise to determine who is liable when damage is caused. AI is heavily reliant on the data that it is trained on, as it makes predictions based on that data, so if the data is flawed, the accuracy of the output is affected, and there could be errors compounded by other errors (e.g. in addition to flawed datasets for training, the algorithm was not a suitable one).

Criminal liability

Our criminal laws presently do not attribute liability to AI systems directly. Criminal liability presently only attaches to natural or legal persons, of which an AI system is not. Where an AI system causes damage, or breaks a criminal law, it would warrant an inquiry into how this arose, and it would turn on the facts whether the programmer of the system, its owner, the person who operated it, or any other person, is criminally liable. The mental state of the human in operating or overseeing the system is a key determining factor – was the consequence something they intended or knew about?

For example, if a person uses an AI system to deliberately commit crimes (contrary to what the AI system was designed for), such as hacking, that person could potentially be found guilty of an offence under the Computer Misuse Act 1993.

The Singapore Academy of Law's Law Reform Committee has issued a "Report on Criminal Liability, Robotics and AI Systems" in February 2021 to explore these issues in-depth, and cautioning that there is no "one size fits all" approach to the application of criminal liability across all uses of AI.

6. Who is responsible for any harm caused by an AI system? And how is the liability allocated between the developer, the user and the victim?

The person responsible for the harm caused by an AI system would depend on the facts of the case, and if there is a contract between the parties, what is set out in the contract.

For example, if the user did not use the AI system for its intended purpose, but for a different purpose despite clear warnings from the developer about the limitations of the AI system, then the developer may not be held responsible for any harm caused. Similarly, if a victim dashed across the road in front of an autonomous vehicle without checking for traffic, he or she may be found contributorily negligent.

The Bioethics Advisory Committee, in its May 2023 consultation paper on *Ethical, Legal and Social Issues Arising from Big Data and Artificial Intelligence Use in Human Biomedical Research*, has also made recommendations on how responsibility for an AI system's wrong decisions should be attributed (at [13.13]):

- AI algorithm researchers – if the root cause of the erroneous decision is found within the original AI research algorithm used to build the model (e.g. erroneous code that was widely disseminated);
- Biomedical researchers – if the cause of the error is due to erroneous adaptation of the original AI research algorithms (e.g. inappropriate AI model construction with said algorithms);
- Developers – if the AI model used to develop the final AI application was erroneously deployed;
- Clinicians – if the AI model is used without adequate evaluation of clinical evidence and was applied for the wrong clinical indication.

7. What burden of proof will have to be satisfied for the victim of the damage to obtain compensation?

In civil cases, the burden of proof is on the balance of probabilities. Where the victim alleges negligence on the part of the defendant AI developer/operator, the victim must establish that there the defendant owed it a duty of care, there was a breach of that duty (falling below a standard of care), and that the breach caused the loss, where the loss is not too remote.

In criminal cases, the case must be proven by the prosecution beyond reasonable doubt. What must be proven depends on the actus reus and mens rea elements of the offence set out in legislation.

8. Is the use of artificial intelligence insured and/or insurable in your jurisdiction?

For the use of autonomous vehicles, it is a requirement that the person authorised to undertake the trial or use of the vehicle must have in place liability insurance indemnifying the owner and any authorised driver or operator of the vehicle in relation to death, bodily injury or damage to property caused by, or arising out of, the use of the vehicle on a road. In lieu of such liability insurance, the person must deposit with the authority a security of not less than SGD$1.5 million, so that the victim will always have a remedy. For more details, please see section 6C of the Road Traffic Act, and rules 14 and 15 of the Road Traffic (Autonomous Motor Vehicles) Rules 2017.

For the deployment of AI technology in other products or services, whether insurance is required is determined by the existing statutory regime for that product or service, and not whether AI is being used.

Nonetheless, developers and users of AI systems are free to consult insurance providers and obtain their own coverage.

9. Can artificial intelligence be named an inventor in a patent application filed in your jurisdiction?

Under Singapore law, the inventor must be the "actual deviser" of the invention (see section 2(1) of the Patents Act 1994), and this must be a natural person (see the cases of *National University Hospital (Singapore) Pte Ltd v Cicada Cube Pte Ltd* [2017] SGHC 53 at para 51, and *Energenics Pte Ltd v Musse Singapore Pte Ltd and anor* [2013] SGHCR 21 at para 24).

It has not yet been tested whether AI may be named as an inventor or joint inventor in Singapore. Across the world, it remains to be seen how regulators will address inventions that are generated by an AI system without any material human input or direction.

10. Do images generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to?

This is an issue that regulators around the world are still examining, and who is the "author" where it comes to content generated by generative AI has not yet been tested in the Singapore courts. In the Discussion Paper on Generative AI released by IMDA in June 2023, whether the current legal landscape surrounding copyright and IP meaningfully addresses the issue of ownership of the content generated by AI was described as an "open debate". [1] In the meantime, it should be addressed with first principles.

Singapore's Copyright Act 2021 requires the author to be a natural person, and for a work to be protected by copyright, it must be original (see Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd [2011] SGCA 37).

Therefore, whether there is copyright over an image generated by/with artificial intelligence likely depends on the level of input the human had when entering the prompt to generate the image. If the human merely prompted "draw a picture of a monkey", it is unlikely to be protected. However, if the human were to give commands on the pose and facial expression of the monkey, the background and other elements of the picture, as well as the style of the image (pencil, watercolour, 3D), it is more likely to be protected by copyright. The answer would be highly dependent on how the AI tool operates and how it is used to create the image.

The IMDA has given further guidance in this regard in the June 2023 paper, stating that current copyright laws protect expression, but not underlying facts, data, ideas or concepts, so "generative AI that now seeks to mimic style, flourishes, curation and creative aspects of the content operates in a grey area, where it is questionable whether these are expressions that are protected". [2]

In the case of autonomous AI-generated work, this has not yet been recognised by any country and Singapore is unlikely to be the first to do so. [3]

Footnotes:

1. Page 12 of the Discussion Paper
2. Page 12 of the Discussion Paper
3. https://www.channelnewsasia.com/singapore/ai-art-copyright-law-artificial-intelligence-authorship-originality-3339396

11. What are the main issues to consider

when using artificial intelligence systems in the workplace?

The Model Framework sets out 4 key areas where organisations should adopt measures to promote the responsible use of AI:

a. Adapt existing or set up internal governance structures and measures to have appropriate oversight over how AI technologies are used in the business; to minimise risks and allocate responsibilities relating to algorithmic decision-making;
b. Determine the appropriate level of human involvement in AI-augmented decision-making based on the organisation's risk appetite for the use of AI and the nature of the decision to be made;
c. Operations management, such that the organisation addresses potential issues when developing, selecting and maintaining AI models, including the management of data (e.g. ensuring it is drawn from representative sources);
d. Strategies for interacting and communicating with stakeholders (e.g. to inform them that AI is being used and how it affects them).

Separately, if an organisation is using generative AI to enhance productivity (e.g. employees use a ChatGPT-like AI system to generate marketing materials, summarise documents), the organisation should have in place guidelines for employees on the use of such tools, and ensure that employees are aware of the limitations of such technology. For example, the organisation should require employees to check the output of the AI system for accuracy, and warn them not to input sensitive data into the system unless the necessary security measures are in place.

12. What privacy issues arise from the use of artificial intelligence?

Artificial intelligence trains and operates on a vast amount of data, which is likely to include personal data. Personal data could be obtained from a broad range of sources (e.g. CCTV cameras, GPS location data, computing devices) and may be obtained from the data subject or another individual (e.g. where applications like ChatGPT are used, the user could input another individual's personal data in the prompt). Data from multiple sources can also be combined to generate insights about a particular individual (e.g. their preferences, buying patterns, emotional state, health status, likelihood of repaying a loan on time). This gives rise to data privacy issues such as whether the data subjects are adequately informed of what personal data will be collected and how the AI system may use and disclose their personal data, as well as whether individuals can prevent use and disclosure or ensure that the data / inferences are accurate.

The Personal Data Protection Act 2012 ("**PDPA**") must be complied with where personal data is processed, whether for the development or in the deployment of the AI system. Please see S/N 13 below.

Organisations can consider the feasibility of using anonymised data, which will not be subject to the PDPA. However, even if a data set is initially anonymised, organisations should be mindful that the risk of re-identification could increase over time (e.g. as the AI system aggregates more data to derive correlations).

13. What are the rules applicable to the use of personal data to train artificial intelligence systems?

The Personal Data Protection Act 2012 ("PDPA") applies to the use of personal data to train AI systems. An organisation that is a data controller (i.e. it determines the purposes and means for processing the personal data, as opposed to taking instructions from another organisation) must adhere to the obligations in the PDPA to safeguard personal data. In brief, the 10 data protection obligations under the PDPA are as follows:

a) Accountability obligation – making information about data protection policies, practices and complaints practices available, designating a Data Protection Officer ("DPO"), and making the DPO's business contact information available to the public;

b) Notification obligation – to notify individuals of the purposes for which the organisation (AI system) will be collecting, using or disclosing their personal data;

c) Consent obligation – only collecting, using or disclosing personal data for purposes which an individual has given his/her consent to, and allowing the individual to withdraw consent.

There are other legal bases for the collection, use and disclosure of personal data (i.e., exceptions to consent that apply in specific circumstances), which are set out in the First and Second Schedules to the PDPA.

For example, the PDPA has exceptions to consent for business improvement purposes. Examples of business improvement purposes include[6]:

a. improving or enhancing goods and services provided, or developing new goods and services to be provided, by the organisation;
b. learning about and understanding the behaviour and preferences of the individual or another individual in relation to the goods or services provided by the organisation;
c. identifying any goods and services provided by the organisation that may be suitable for the individual or another individual, or personalising or customising any such goods or services for the individual or another individual.

The organisation also has to satisfy the conditions prescribed for the respective legal bases, e.g., an organisation may rely on the business improvement exception only if the organisation's business improvement purposes cannot reasonably be achieved without using the personal data in individually identifiable form (among other conditions);

d) Purpose Limitation obligation – to only collect, use or disclose personal data for purposes that a reasonable person would consider appropriate under the given circumstances;

e) Accuracy obligation – to make reasonable efforts to ensure that the personal data collected is accurate and complete, if it is likely to be used to make a decision that affects the individual or to be disclosed to another organisation;

f) Protection obligation – to make reasonable security arrangements to protect the personal data in the organisation's possession to prevent unauthorised access, collection, use, disclosure, modification, disposal or similar risks;

g) Retention Limitation obligation – to cease retaining personal data or dispose of it in a proper manner when it is no longer needed for any business or legal purpose;

h) Transfer Limitation obligation – to transfer personal data to another country outside Singapore only in accordance with the requirements prescribed under the PDPA, to ensure that the standard of protection accorded to the transferred data is comparable to the PDPA;

i) Access and Correction obligation – upon request, to provide individuals with access to their personal data as well as information about how the data was used or disclosed within a year before the request, and to correct any error or omission in the personal data and send the corrected data to other organisations to which the personal data was disclosed within a year before the correction is made;

j) Data Breach Notification obligation – where a data breach is likely to result in significant harm, the organisation must notify the PDPC and affected individuals. Further, if a data breach is of significant scale, the organisation must notify the PDPC.

In contrast, an organisation that is a "data intermediary" (i.e. one that processes personal data on behalf of another organisation pursuant to a written contract) is subject only to the Protection and Retention Limitation obligations, with an additional obligation to notify the organisation for which it is processing personal data of a data breach without undue delay under the Data Breach Notification obligation.

Where there are different parties involved in the development or deployment of the AI system, there can be complexity in determining who is the controller or data intermediary, which may vary depending on the system and at different stages. The precise roles and responsibilities of each party should therefore be clearly set out in contract. For example, a service provider, which is developing and deploying an AI system for its customer, may be a data intermediary where it processes personal data on behalf of the customer on its instructions for these purposes. However, where the service provider retains and uses the personal data to improve the performance of its AI system for its own purposes, it may be a controller.

Footnotes:

1. See Division 2 of Part 2 of the Second Schedule to the PDPA.

14. Have the privacy authorities of your jurisdiction issued guidelines on artificial intelligence?

The PDPC has issued the following guidance to assist the industry with navigating AI:

a. 5 June 2018: PDPC published a Discussion Paper on AI and Personal Data – Fostering Responsible Development and Adoption of AI, which was their preliminary analysis of issues pertinent to the commercial development and adoption of AI solutions;
b. January 2019: IMDA/PDPC published the 1st edition of the Model Framework
c. January 2020: IMDA/PDPC published the 2nd edition of the Model Framework

In the later part of 2023 (as announced by the Ministry of Communications and Information on 9 April 2023), the PDPC will issue advisory guidelines on the use of

personal data in AI systems under the PDPA.[1]

Footnotes:

1. https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2023/5/mci-response-to-pq-on-ensuring-development-and-maintenance-of-ethical-artificial-intelligence-standards?category=Cyber+Security

15. Have the privacy authorities of your jurisdiction discussed cases involving artificial intelligence?

The PDPC has not yet published any enforcement decision or released any statement on specific cases involving the processing of personal data with artificial intelligence.

16. Have your national courts already managed cases involving artificial intelligence?

Singapore's courts have not yet issued decisions on cases involving artificial intelligence.

However, our Court of Appeal has issued a landmark decision on the use of deterministic algorithms to conclude contracts in the case of *Quoine Pte Ltd v B2C2 Ltd* (2020) SGCA(I) 02. A deterministic algorithm is one that "will always produce precisely the same output given the same input […] and does not have the capacity to develop its own responses to varying conditions" (see [15]). Therefore, where an attempt is made to void contracts concluded by such algorithms for unilateral mistake, in order to determine knowledge of that mistake, the court will refer to the state of mind of the algorithm's programmers from the time of programming up to the point where the relevant contract is formed (see [97] to [99]).

It will be interesting to see whether the same principles apply where the algorithm is non-deterministic (i.e. it can learn from the data input into it and thus modify its behaviour), or if there are multiple programmers, as the software used by B2C2 was devised almost exclusively by one of its founders.

17. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence?

The IMDA plays a key role in promoting the responsible adoption of AI across the public and private sectors. It has issued the Model Framework that applies across all sectors, as well as developed AI Verify, an AI governance testing framework and a software toolkit, amongst other initiatives.

The Smart Nation and Digital Government Office (SNDGO), which drives the digital transformation of the government, issued Singapore's National AI Strategy in 2019. A National AI Office was also established under the SNDGO in order to set the national agenda for AI, as well as partner the research community and industry to implement the National AI Strategy.

However, the SNDGO and IMDA do not act alone. Regulators in other sectors also issue guidelines on the use of AI for their sectors (e.g. health, finance, etc.).

18. How would you define the use of artificial intelligence by businesses in your jurisdiction? Is it widespread or limited?

The use of AI by businesses in Singapore is gaining momentum. In IBM's Global AI Adoption Index 2022, which surveyed 500 business decision makers in Singapore, 39% of them indicated that their organisations have deployed AI, and another 46% indicated that their organisations were looking to do so. [1]

In Microsoft's annual Work Trend Index report (issued 31 May 2023), Microsoft reported that LinkedIn data from Singapore showed that the number of persons holding AI job roles between 2016 and 2022 grew by 565%, outpacing countries like Australia, India and Japan, and outpaced the growth in overall hiring by 14% in 2022. [2]

To aid businesses in deploying AI solutions in the workplace, our regulators have also issued "A Guide to Job Redesign in the Age of AI", where "jobs" should be broken down into "tasks", as AI impacts on how tasks are to be performed. The guide also sets out considerations for deciding whether a task should be automated.

Footnotes:

1. https://www.ibm.com/downloads/cas/GVAGA3JP
2. https://news.microsoft.com/en-sg/2023/05/31/microsoft-work-trend-index-2023-singapore-data-unveils-opportunities-to-unlock-workplace-productivity-and-creativity-in-the-age-of-ai/

19. Is artificial intelligence being used in the legal sector, by lawyers and/or in-house counsels? If so, how?

The legal sector is already using AI in a variety of ways, such as for discovery in litigation, and for due diligence processes in M&A transactions (e.g. to detect patterns across contracts and highlight differences between them). With the accessibility of generative AI tools like ChatGPT, the legal sector is also starting to explore how to integrate such tools into their workflows such as for research or document generation.

20. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

Of the 5 challenges set out, 3 relate to the developing landscape on how this new technology should be regulated, as there is no one-size-fits-all solution. The other 2 are changes to the nature of legal practice. We have chosen to address the challenges and opportunities together, since the challenges are actually opportunities to clarify the law and also ensure the legal profession keeps pace with technological developments.

1. Because this is a developing field both in Singapore and overseas, it is important for lawyers to keep abreast of overseas developments, as technology can be exported across international borders. The pace at which legislation and guidelines are issued across the world has increased exponentially in 2023, and lawyers must remain up to date on these latest developments.
2. AI can be deployed in so many ways, so there is no one-size-fits-all solution (or regulation), and lawyers must be keenly aware of this. The rules surrounding AI used in a music recommendation system will be different from that in a system used by a bank to determine if a person should be granted a loan, because of the gravity of their impact on a person. The challenge will be in calibrating the level of governance measures/precautions to be taken in each scenario, without exposing the organisation to unnecessary (legal and other) risk.
3. Determining liability where the AI system causes damage, or does not perform as expected. Lawyers must be aware of whether there are features of AI that make it different from other technologies, and assess whether there may be limitations in applying existing legal principles and how to overcome them. AI systems learn from the data they are trained on and can improve with the experience without being explicitly programmed. Aside from having an 'autonomous' quality (where their outcome may not always be foreseen), the quality of the data used to train the system also matters, as well as how different the real-world data input into the system is from the training data, as that also affects the AI system's performance.
4. The nature of the work performed by lawyers will change as Large Language Models like ChatGPT are increasingly incorporated into legal practice, in tandem with other AI tools. Lawyers must understand the technology so that they can decide how to harness it in their work (including taking precautions for client confidentiality and checking the content generated by generative AI tools), and explain its use to their clients.
5. There is an increasing demand from the public for legal AI tools for laypersons to use so they can access the law on their own. Lawyers will have to address issues such as where to draw the line where generative AI is giving legal information versus giving legal advice, and also who is to assume liability if the advice/information rendered is incorrect.

21. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months?

Singapore takes a practical, balanced approach towards the regulation of artificial intelligence. As at June 2023, our regulators have announced that they are currently not looking implement any general AI legislation. Instead, Singapore will focus on promoting the responsible use of artificial intelligence in the industry. However, Singapore will still be keeping a close eye on developments overseas.

Therefore, over the next 12 months, we will likely see our regulators issuing more guidelines to the industry in their specific sectors (e.g. using AI to process personal data, which is slated to be released later this year), together with more public consultations. Relevant use cases of AI will also be analysed. Our regulators have indicated that no person has all the answers where it comes to regulating this space, hence they will be working closely with the industry to understand the benefits and challenges of AI across a spectrum of use cases before deciding on the regulatory approach.

Testing and evaluation measures (AI Verify) will continue to be developed, with much industry feedback. Testing is a very significant landmark on the road to legislation (if assessed to be necessary), so that legislation can be enforced. After all, if the use of AI must fulfil criteria A, B and C, there must be an objective means to tell that the criteria have been fulfilled.

Contributors

Lim Chong Kin
Managing Director
chongkin.lim@drewnapier.com

Anastasia Su-Anne Chen
Director
anastasia.chen@drewnapier.com

Cheryl Seah
Director
cheryl.seah@drewnapier.com