



AI, Machine Learning & Big Data 2025

Seventh Edition

Contributing Editor:

Charles Kerrigan

CMS LLP

glg Global Legal Group

TABLE OF CONTENTS

Preface

Charles Kerrigan
CMS LLP

Expert Analysis Chapters

- 1** **Autonomous AI: Who is responsible when AI acts autonomously and things go wrong?**
Erica Stanford
CMS LLP
- 11** **Profiling and prohibited practices: A summary of legal requirements for automated decision-making in the EU and UK**
Lisa McClory
CMS LLP
- 19** **Practical guidelines for the use of generative AI**
David V. Sanker
SankerIP
- 27** **The role of multilateralism in AI**
Emma Wright
Interparliamentary Forum on Emerging Technologies

Jurisdiction Chapters

- 31** **China**
Ian Liu, Andy Yu, Timothy Chow & Helen Xie
Deacons
- 43** **Cyprus**
Christiana Aristidou & Evdokia Marcou
The Hybrid LawTech Firm, empowered by Christiana Aristidou LLC
- 53** **Czech Republic**
Jana Pattynová & Karina Matevosjanová
Pierstone
- 59** **Estonia**
Sander Peterson
Magnusson Estonia
- 68** **France**
Boriana Guimberteau & Elise Dufour
Stephenson Harwood
- 82** **Germany**
Dr. David Bomhard & Dr. Jonas Sigmüller
Aitava

- 91 Greece**
Marios D. Sioufas
Sioufas & Associates Law Firm
- 108 Hong Kong**
Dominic Wai & Lawrence Yeung
ONC Lawyers
- 117 Ireland**
Jane O’Grady & Victor Timon
Byrne Wallace Shields LLP
- 129 Italy**
Massimo Donna
Paradigma – Law & Strategy
- 142 Japan**
Akira Matsuda, Ryohei Kudo & Taiki Matsuda
Iwata Godo
- 154 Malta**
Ron Galea Cavallazzi & Alexia Valenzia
Camilleri Preziosi
- 163 Mexico**
Alfredo Lazcano & Andrea Avedillo
Lazcano Sámano, S.C.
- 169 Netherlands**
Joris Willems & Danique Knibbeler
NautaDutilh
- 182 Poland**
Michał Nowakowski, Martyna Rzeczkowska & Paulina Grzywacz
ZP Zackiewicz & Partners
- 199 Singapore**
Lim Chong Kin, Anastasia Su-Anne Chen & Cheryl Seah
Drew & Napier LLC
- 213 Switzerland**
Jürg Schneider & David Vasella
Walder Wyss Ltd.
- 223 Taiwan**
Robin Chang & Eddie Hsiung
Lee and Li, Attorneys-at-Law
- 234 Türkiye**
Burak Özdağıştanlı, Hatice Ekici Tağa, Sümeyye Uçar & Begüm Alara Şahinkaya
Ozdagistanli Ekici Attorney Partnership

239 United Arab Emirates

Aman Garg, Abhinesh Takshak & Parth Singh

Node.Law

250 United Kingdom

Charles Kerrigan, Erica Stanford, Lisa McClory & Ben Hitchens

CMS LLP

263 USA

Ryan Abbott, Timothy Lamoureux & Kumiko Kitaoka

Brown, Neri, Smith & Khan, LLP

Singapore

Lim Chong Kin
Anastasia Su-Anne Chen
Cheryl Seah

Drew & Napier LLC

Trends

Artificial intelligence (“AI”), big data and machine learning have been the subject of tremendous interest in Singapore in recent years. Advances in mobile computing and increasingly widespread internet and social media usage, among other factors, have contributed to the availability of large volumes of data, which are increasingly being analysed by machine-learning algorithms to make predictions or decisions.

The adoption of AI has been identified by the Government as one of the nine key trends that will move the digital economy in Singapore over the next three to five years.¹ In 2019, the Government launched a National Artificial Intelligence Strategy, aiming to establish Singapore as a leader in developing and deploying scalable, impactful AI solutions in sectors that are highly valuable and pertinent to both citizens and businesses by 2030.² There will be an initial tranche of five “National AI Projects” in the high socio-economic impact sectors of border security, logistics, healthcare, education management and estate management.

In 2023, the renewed National Artificial Intelligence Strategy 2.0 was launched, where AI is now seen as a “necessity” rather than just “good to have”. Singapore will ensure that its population understands how to harness AI effectively, while at the same time taking differentiated approaches to manage the risks to and from AI, ranging from regulatory moves to voluntary guidelines.³

Key initiatives to build Singapore’s AI capabilities include:

- (a) the 2017 launch of AI Singapore, a National AI programme which aims to enhance Singapore’s AI capabilities, nurture local talent and build an ecosystem of AI start-ups and companies developing AI products;
- (b) the provision of Government grants and incentives, such as the AI and Data Analytics (“AIDA”) Grant offered by the Monetary Authority of Singapore (“MAS”), which aims to promote the adoption and integration of AIDA in financial institutions, as well as a \$150 million Enterprise Compute Initiative (announced in the Government’s 2025 Budget) for eligible companies to be partnered with major cloud service providers to access AI tools and computing power, together with expert consultancy services;⁴ and

- (c) the launch of the AI Verify Foundation in June 2023, comprising members from both government and industry, to develop AI testing tools to promote the responsible use of AI.⁵

Various governmental and regulatory agencies have also issued policy papers setting out their views on matters relating to AI and big data, and have invited stakeholder feedback on certain policy issues and proposals by way of consultation exercises. Recent examples include:

- (a) the Infocomm Media Development Authority (“IMDA”) and Personal Data Protection Commission’s (“PDPC”) Model Artificial Intelligence Governance Framework (“Model AI Framework”). The Model AI Framework is the first in Asia and is intended to provide guidance to private sector organisations for the purpose of addressing key ethical and governance issues that may arise from their deployment of AI solutions;
- (b) a research paper titled “Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights”, published by the Competition & Consumer Commission of Singapore (“CCCS”, formerly the Competition Commission of Singapore) in collaboration with the Intellectual Property Office of Singapore (“IPOS”);
- (c) the “Principles to Promote Fairness, Ethics, Accountability and Transparency (“FEAT”) in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector”, issued by the MAS, provide a set of generally accepted principles for the use of AIDA in decision-making related to providing financial products and services;
- (d) the MAS’s Veritas Initiative, which will enable financial institutions to evaluate their AIDA solutions against the FEAT principles;⁶
- (e) the PDPC’s publication of Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems on 1 March 2024 (“PDPC’s Guidelines on AI”); and
- (f) the IMDA and AI Verify Foundation’s joint publication of the Model AI Governance Framework for Generative AI on 30 May 2024, which sets out key issues for the public and policymakers to address, spanning misinformation to accountability across the AI development chain to intellectual property (“IP”) infringement.

Internationally, Singapore has also entered into agreements with other nations⁷ to strengthen and develop AI research and collaboration efforts. In October 2023, Singapore and the US made efforts to deepen cooperation in AI by making their AI governance frameworks interoperable (mapping Singapore’s AI Verify to the US NIST AI Risk Management Framework), establishing a bilateral AI Governance Group and pledging to increase exchanges and programmes to deepen research and technical collaborations in AI.⁸ Singapore has since continued to align our AI governance testing framework with other countries, mapping the AI Verify Framework to the newly-launched ISO/IEC 42001:2023 so that companies may practically demonstrate alignment with the ISO standard without onerous cost.⁹

In terms of wider efforts in the region, the Association of Southeast Asian Nations’ (“ASEAN”) Guide on AI Governance and Ethics was published in February 2024 to provide practical guidance for organisations in the region that wish to design, develop and deploy traditional AI technologies in commercial and non-military or dual-use applications.¹⁰ This guide was enhanced in January 2025 with the release of the Expanded ASEAN Guide on AI Governance and Ethics – Generative AI, which sets out the opportunities and risks of generative AI and recommended policy actions for ASEAN to adopt generative AI responsibly.¹¹ Singapore, together with Rwanda, has also led an initiative amongst the Digital Forum of Small States to publish the AI Playbook for Small States in September 2024 – an anthology of best practices from members on how they have each implemented AI strategies and overcome challenges particular to small states (e.g. limited resources, access to data and talent, and small domestic markets).¹²

The Singapore courts have also had the opportunity to address issues raised by the use of algorithms in the context of cryptocurrency. In the case of *B2C2 Ltd v Quoine Pte Ltd* [2019] 4 SLR 17 (“*B2C2 v Quoine*”),

the Singapore International Commercial Court (“SICC”) had to determine the appropriate application of legal principles to a cryptocurrency exchange where trading was conducted via an algorithmic system as opposed to direct human action.

The algorithmic program in *B2C2 v Quoine* was found by the SICC to be “deterministic” in nature, with “no mind of [its] own”, but “[a] mere machine [...] carrying out actions which in another age would have been carried out by a suitably trained human”. However, the SICC (per Simon Thorley J) opined that the ascertainment of knowledge in cases where computers have replaced human action will develop in the future as disputes arise as a result of such action, particularly in cases where the computer in question is “creating artificial intelligence” and can be said to have “a mind of its own” (*B2C2 v Quoine* at [206] to [209]). This was affirmed by the majority of the Court of Appeal on appeal, in *Quoine Pte Ltd v B2C2 Ltd* [2020] 2 SLR 20.

More recently, the Supreme Court of Singapore also issued a Guide on the Use of Generative AI Tools by Court Users, which sets out steps that lawyers and litigants-in-person must adhere to when using generative AI tools to prepare court documents.¹³

Ownership/protection

The Singapore Government has sought to facilitate the protection of IP rights in AI technologies, to help innovative enterprises bring AI products to market faster. As the IP landscape is still evolving, especially where it comes to the use of copyrighted materials for training generative AI systems, on 28 February 2024, IPOS, together with the Singapore Management University Centre for AI & Data Governance, published a report titled “When Code Creates: A Landscape Report on Issues at the Intersection of Artificial Intelligence and Intellectual Property Law”, which collates the treatment of selected key IP issues across various jurisdictions.¹⁴ Some of these pertinent issues are discussed below.

Protection for AI technologies

Under section 13 of the Patents Act 1994, for an invention to be patentable, it must satisfy three conditions:

- (a) the invention must be new;
- (b) involve an inventive step; and
- (c) be capable of industrial application.

Companies considering the possibility of patent protection for AI inventions may wish to note that potential issues may arise because mathematical methods, i.e., algorithms *per se*, are not considered inventions, and solving a generic problem such as using the method in controlling a system is unlikely to cross the threshold.

That said, IPOS also stated in its IP and Artificial Intelligence Information Note that where the patent application relates to the application of a machine learning method to solve a specific problem in a manner that goes beyond the underlying mathematical method, the application could be regarded as an invention.¹⁵

Apart from the protection of AI solutions under patent law, the source code of a computer program may also be protected by copyright. Section 13(1)(b) of the Copyright Act 2021 expressly provides that “literary work” includes a “computer program” for the purposes of the Copyright Act 2021.

In the context of AI, a couple of further issues may become increasingly relevant. These are: (i) rights in relation to data; and (ii) rights in relation to works generated by AI.

Exception for text and data mining

The Singapore Government has observed, in the Singapore Copyright Review Report (issued 17 January 2019), that text and data mining and its applications are crucial elements that fuel economic growth and

support Singapore's drive to catalyse innovation in the digital economy. Text and data mining refers to the use of automated techniques to analyse text, data and other content to generate insights and information. However, those involved in such activities risk infringing copyright law, as the initial phase of the work typically involves incidentally extracting or copying data from large quantities of material that may be protected by copyright.

In this light, section 244 of the Copyright Act 2021 allows the copying of copyrighted materials for the purpose of computational data analysis, including for the development and verification of machine learning models, provided that certain conditions are satisfied. One such condition involves the user having lawful access to the materials that are copied (e.g. not to circumvent paywalls). Notably, the exception in question does not distinguish between commercial and non-commercial use.

Protection of AI-generated works

At this juncture, it remains to be seen how IP laws may be applied to protect AI-generated works. Under the present IP legal framework, a number of issues are likely to arise with respect to the protection of AI-generated works. Programs capable of generating such works already exist and are in use. For instance, natural language processing models, such as ChatGPT, are frequently used by students and organisations to generate content.¹⁶

The Singapore courts have recognised that, under existing Singapore copyright law, only natural persons may be considered authors of works, although legal persons, like companies, may own the copyright in works. It is therefore necessary to be able to attribute the creative elements of a work to a natural person in order for copyright to vest.¹⁷ Under the present statutory regime, the courts have further observed that “in cases involving a high degree of automation, there will be no original work produced for the simple reason that there are no identifiable human authors”,¹⁸ where authorship is defined in terms of the exercise of independent, original or creative intellectual efforts.¹⁹

Antitrust/competition laws

The Competition Act 2004 (“Competition Act”) establishes a general competition law in Singapore. The Competition Act generally prohibits:

- (a) anti-competitive agreements (the section 34 prohibition);²⁰
- (b) the abuse of a dominant position (the section 47 prohibition);²¹ and
- (c) mergers and acquisitions that substantially, or may be expected to substantially, lessen competition within any market in Singapore (the section 54 prohibition).²²

The CCCS is the statutory authority responsible for administering and enforcing the Competition Act.

Competition issues pertaining to AI and big data have been the subject of various studies²³ by the CCCS.

Anti-competitive agreements and concerted practices facilitated by algorithms

Among the topics discussed in one of the CCCS's papers²⁴ is anti-competitive agreements and concerted practices facilitated by algorithms.

In the paper, the CCCS recognised the need to balance efficiency gains against the increased risk of collusion. In this regard, the CCCS has identified several concerns in relation to algorithms providing new means of fostering collusion. First, monitoring algorithms may enhance market transparency and organisations may be able to automatically extract and evaluate real-time information concerning the prices, business decisions and market data of competitors. Second, algorithms increase the frequency of interaction between organisations and the ease of price adjustments, as automated pricing algorithms may be able to automate the decision process of colluding organisations so that prices react simultaneously

and immediately to changes in market conditions.²⁵ The CCCS has announced (in September 2024) that it is developing a tool for companies to use in testing their AI systems for any potential anticompetitive behaviour.²⁶

The CCCS has identified certain concerns about whether the existing competition enforcement framework is adequately equipped to deal with future developments involving algorithms. The main concern lies in how algorithms may lead to greater instances of tacitly collusive equilibriums (i.e., collusive agreements being reached without any explicit communication between competitors) that may fall outside the current scope of competition enforcement.²⁷

Board of directors/governance

On 21 January 2020, the IMDA/PDPC published the second edition of its Model AI Framework.²⁸ The Model AI Framework sets out common definitions and principles relating to the responsible use of AI. Adoption of the Model AI Framework is on a voluntary basis.

The Model AI Framework comprises guidance on four key areas, including organisations' internal governance structures and measures. The Model AI Framework also expressly recognises that “[t]he sponsorship, support, and participation of the organisation's top management and its Board in the organisation's AI governance are crucial”. One of the suggested practices includes establishing a coordinating body that has relevant expertise and proper representation from across the organisation to oversee the ethical deployment of AI.

Briefly, the principles set out in the Model AI Framework across the four key areas include the following:

- (a) Internal governance structures and measures: organisations should ensure that there are clear roles and responsibilities in place for the ethical deployment of AI, as well as risk management and internal control strategies.
- (b) Determining AI decision-making models: organisations should consider the risks of using a particular AI model based on the probability and severity of harm and determine what degree of human oversight would be appropriate based on the expected probability and severity of harm.
- (c) Operations management: organisations should take steps to understand the lineage and provenance of data, and the quality of their data, as well as the transparency of the algorithms chosen.
- (d) Stakeholder interaction and communication: organisations should take steps to build trust and maintain open relationships with individuals regarding the use of AI, including steps such as general disclosure, increased transparency, policy explanations and careful design of human–AI interfaces.

Complementing the Model AI Framework is the Implementation and Self-Assessment Guide for Organisations, a companion guide that aims to help organisations assess the alignment of their AI governance practices with the Model AI Framework, as well as the Compendium of Use Cases, which features organisations that have implemented accountable AI practices.

In order to assure the public that AI systems are fair, explainable and safe, Singapore launched AI Verify in May 2022, a self-assessment AI governance testing framework and toolkit for organisations containing both software for technical tests and a series of questions for process checks. AI Verify does not use pass-fail standards, but enables organisations to be more transparent about the performance of their AI systems.²⁹ The AI Verify Foundation was subsequently launched in June 2023 with the goal of boosting AI testing capabilities to meet the needs of companies and regulators globally.³⁰

On 30 May 2024, the AI Verify Foundation and IMDA launched the Model AI Governance Framework for Generative AI.³¹ The framework expanded on the existing Model AI Framework, which only covers “Traditional AI” (which makes predictions based on existing/historical data instead of creating new content), by proposing nine dimensions to support a comprehensive and trusted Generative AI ecosystem.

Regulations/government intervention

At present, Singapore does not have legislation governing the use of AI in general (unlike the proposed EU AI Act), but has voluntary guidelines for individuals and businesses, such as the Model AI Framework.

Protection of personal data

The use of datasets in conjunction with AI applications has the potential to raise data protection (“DP”) issues, especially where such datasets contain personal data.

The Personal Data Protection Act 2012 (“PDPA”) sets out the general DP framework, which governs the collection, use and disclosure of personal data by private sector organisations in Singapore. It operates alongside sectoral laws and regulations, such as those issued by the MAS for the financial sector.

Under the PDPA’s general DP framework, there are presently 10 main obligations, with one more obligation (i.e., the Data Portability Obligation) to come into force in the future. Since the enactment of the PDPA, the general DP framework has largely operated as a consent-based regime. In this regard, the “consent obligation” under the PDPA requires an organisation to obtain an individual’s consent before the collection, use or disclosure of personal data, unless an exception applies.³²

Importantly, the amendments to the PDPA under the Personal Data Protection (Amendment) Act 2020 introduced numerous revisions to the consent framework, including recognising the presence of deemed consent under certain circumstances, as well as expanding the range of the exceptions to consent under the PDPA, so as to empower businesses to use data for innovation.

In the PDPC’s Guidelines on AI, the PDPC encourages the use of anonymised data, as far as possible. Anonymised data is no longer personal data (and therefore not governed by the PDPA). According to the PDPC’s Advisory Guidelines on the PDPA for Selected Topics, data would be considered anonymised if there is no serious possibility that an individual could be re-identified, taking into consideration both:

- (a) the data itself, or the data combined with other information to which the organisation has or is likely to have access; and
- (b) the measures and safeguards implemented by the organisation to mitigate the risk of re-identification.

Organisations would have to be mindful that technological advancements may increase the risk of re-identification of a dataset, which was previously anonymised, and thereby be considered personal data.³³ Organisations would also have to weigh the trade-offs with using anonymised data when developing or training AI systems (such as model accuracy, repeatability or reproducibility of results).³⁴

Cybersecurity

The Cybersecurity Act 2018 establishes the framework for the oversight and maintenance of national cybersecurity in Singapore and imposes duties and obligations on computer systems designated as critical information infrastructure (“CII”). The Cybersecurity Act 2018 operates alongside the Computer Misuse Act 1993 (“CMA”), which criminalises cyber activities such as hacking, denial-of-service attacks, infection of computer systems with malware, and other sector-specific regulatory frameworks. On 11 April 2022, the licensing framework for cybersecurity service providers came into effect,³⁵ along with the Cybersecurity (Cybersecurity Service Providers) Regulations 2022. The licensing framework, which covers cybersecurity service providers offering penetration testing services and managed security operations centre monitoring services, aims to improve the standard of cybersecurity service providers, and address the information asymmetry between such providers and consumers.

The Cybersecurity (Amendment) Act 2024 (“Amendment Act”) was passed in mid-2024, but is yet to come into operation at the time of writing. At the time the Cybersecurity Act 2018 was enacted, providers of essential services tended to own and control the CII used for continuous delivery of the essential services they were responsible for. To keep up with the evolving business landscape, the Amendment Act expands

the Cyber Security Agency of Singapore's ("CSA") oversight beyond CII owners to: (1) essential service providers who use CII owned by a computing vendor; (2) major foundational digital infrastructure service providers (i.e., cloud-computing service providers and data centre facility service providers); (3) entities of special cybersecurity interest; and (4) owners of systems of temporary cybersecurity concern.

Separately, the CSA published the Guidelines and Companion Guide on Securing AI Systems on 15 October 2024, which set out recommended practices for owners of AI systems to follow in order to secure the AI systems throughout their life cycle.³⁶ The guidelines highlight that while AI systems are software systems and vulnerable to classical cybersecurity threats such as supply chain attacks and intrusion or unauthorised access, malicious actors may also employ novel methods of attack such as Adversarial Machine Learning that set out to distort the AI system's behaviour. The Companion Guide provides practical mitigation measures for decision makers, AI practitioners and cybersecurity practitioners to address cybersecurity risks to AI systems.

Protection from Online Falsehoods and Manipulation Act 2019 ("POFMA")

Singapore is one of many jurisdictions to have enacted laws to deal with fake news and misinformation. The POFMA, which came into effect on 2 October 2019, seeks to, among others, prevent the electronic communication of false statements of fact in Singapore. In particular, it is an offence under the POFMA for a person to make or alter an automated computer program (i.e., a "bot") with the intention of using it to communicate false statements of fact in Singapore.

Regulation of autonomous motor vehicles

The Singapore Government has also recognised the potential benefits that AI may bring to the transportation sector and has sought to facilitate trials involving autonomous vehicles. In 2017, the Road Traffic Act 1961 was amended to include specific definitions relating to autonomous vehicles.³⁷

Furthermore, the Road Traffic (Autonomous Motor Vehicles) Rules 2017 ("Autonomous Vehicles Rules") were introduced to regulate the trials of autonomous vehicles. Parties interested in trialling autonomous vehicles must submit an application to the Land Transport Authority ("LTA"). In granting a party the authorisation to conduct these trials, the LTA retains the discretion to impose conditions, such as the autonomous vehicle to be accompanied by a safety driver that has been trained to take full control of the autonomous vehicle when required, and the geographical area in which the trial may be conducted.³⁸

In January 2019, Enterprise Singapore published Technical Reference 68, a set of provisional national standards to guide the industry in the development and deployment of fully autonomous vehicles. Technical Reference 68 promotes the safe deployment of fully autonomous vehicles in Singapore and contains standards for vehicle behaviour, vehicle safety, cybersecurity and data formats.

Generative AI/foundation models

In 2023, the IMDA published a discussion paper titled "Generative AI: Implications for Trust and Governance", which set out six key risks of generative AI and good governance approaches to mitigate those risks.³⁹ This was followed by a second discussion paper, "Cataloguing LLM Evaluations", which sets out baseline evaluation and testing approaches for large language models ("LLMs").⁴⁰

Singapore has recognised the need for a common standard approach to assessing generative AI. The IMDA and AI Verify Foundation launched the first-of-its-kind Generative AI Evaluation Sandbox ("the Sandbox") in October 2023.⁴¹ Through the participation of industry partners and regulators, the Sandbox aims to build up a body of knowledge on how generative AI products should be tested. To date, more than 10 global industry players have joined the Sandbox, including the likes of Google, Microsoft, Anthropic, IBM, NVIDIA, Stability.AI and Amazon Web Services.

In May 2024, the Model AI Governance Framework for Generative AI was released by the AI Verify Foundation and IMDA. The framework sets out actions to be taken across nine dimensions below to address the risks posed by generative AI, while continuing to facilitate innovation.⁴² At the same time, “Project Moonshot”, one of the world’s first evaluation toolkits for LLMs, was released for public use.

Accountability: responsibility should be allocated based on the level of control each person has in the generative AI development chain.

Data used in model training: there is a need for open dialogue and guidance between policymakers and relevant stakeholders on how personal data laws and copyright laws apply to data used in model training.

Trusted development and deployment: there is a need to adopt common safety practices and standardise disclosure about generative AI models to facilitate comparability across models and incentivise safer model use.

Incident reporting: there is a need for AI developers to report safety vulnerabilities in their AI systems and then act pre-emptively to patch the system. Organisations should also report to regulators incidents of a certain severity arising from their use of AI systems.

Testing and assurance: policymakers and international standards organisations (e.g., International Organisation for Standardisation) should develop common standards for AI testing to ensure quality and consistency.

Security: new testing tools must be developed to address the risks specific to generative AI.

Content provenance: users should be aware that they are interacting with AI-generated content to reduce the risk of misinformation, so technical solutions such as digital watermarking and cryptographic provenance should be explored, in tandem with public education on verifying the authenticity of content.

Safety and alignment Research & Development (“R&D”): there should be investment in R&D, with more AI safety R&D institutes set up to conduct alignment research in tandem with AI companies. AI safety R&D institutes should cooperate globally to optimise limited resources and keep pace with commercial developments.

AI for public good: Responsible use of AI should go beyond risk mitigation and actively seek to improve people’s lives. Governments should partner companies and communities on digital literacy initiatives, drive innovation in the industry (especially among SMEs), upskill the workforce and redesign jobs, and ensure AI is environmentally sustainable.

Separately, the MAS has partnered with the industry in developing a framework for the responsible use of generative AI in the financial sector under the Project MindForge⁴³ and has published a whitepaper on Emerging Risks and Opportunities of Generative AI for Banks.⁴⁴

Generative AI is also being used to increase access to justice, where it will be used to assist self-represented litigants in the Small Claims Tribunal.⁴⁵

AI in the workplace

With a small and ageing population, the use of AI and automation is necessary for Singapore to preserve its competitive edge over other economies. At present, automation of jobs is being used to combat the shrinking workforce in areas that rely heavily on manual labour, such as sanitation.⁴⁶ The Singapore Government has also introduced measures to encourage the adoption of AI automation, such as through the Enterprise Development Grant.⁴⁷ The IMDA also developed and published “A Guide to Job Redesign in the Age of AI” to help companies manage AI’s impact on employees and prepare for the future of work.⁴⁸

Implementation of AI/big data/machine learning into businesses

As part of facilitating the adoption of AI by businesses, Singapore is also focused on new initiatives to

enhance skillsets in AI among the country's workforce. One government initiative, "AI for Everyone", is freely available to the public and seeks to introduce students and working adults to the potential of AI technologies. Furthermore, Singaporeans can make use of the TechSkills Accelerator programme, a SkillsFuture initiative driven by the IMDA to develop their competencies in the ICT sector, which includes fields such as AI, software development, data analytics and cybersecurity.

Civil liability

The civil liability regime for AI is in its nascent stages in Singapore. The courts are examining how existing legal frameworks (e.g., contractual, tortious, equitable and property law principles) apply to risk and liability issues concerning AI.

For example, in the landmark case of *Quoine Pte Ltd v B2C2 Ltd* [2020] 2 SLR 20, which involved smart contracts and the autonomous algorithmic trading of digital tokens, the existence of a contractual relationship between buyers and sellers when executing a trade on the digital token exchange was recognised by the Court of Appeal. Accordingly, the Court of Appeal applied traditional contractual principles of unilateral mistake and breach of contract to a contractual relationship represented by a smart contract.

In the meantime, studies on the applicability of Singapore law to AI systems are underway, with the Singapore Academy of Law's Law Reform Committee ("LRC") establishing a Subcommittee on Robotics and AI in 2020 to consider and make recommendations on the above. With respect to civil liability, the LRC published the "Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars", proposing and discussing possible frameworks for determining liability on the basis of negligence, strict liability and no-fault liability in the context of self-driving vehicles.

Criminal issues

The CMA

Although not specific to AI, the CMA is the main legislation in Singapore that prescribes a list of criminal offences relating to computer material or services (which may be relevant to AI systems), which includes, among others, unauthorised access (e.g., hacking), unauthorised modification of computer material (e.g., infection of IT systems with malware) and unauthorised obstruction of the use of computers (e.g., denial-of-service attacks).

In 2021, the LRC also published the "Report on Criminal Liability, Robotics and AI Systems", which discusses potential risks posed to humans and property by the use of robotics and AI systems, and examines whether and how Singapore's criminal laws and principles of criminal liability may apply in such situations.

Discrimination and bias

The Model AI Framework sets out principles for the ethical use of AI in the private sector, including addressing problems relating to bias within AI systems by means of:

- (a) training staff dealing with AI systems to interpret AI model output and decisions to detect and manage bias in data; and
- (b) using reasonable effort to assess and manage the risks of inherent bias and inaccuracy of datasets used for AI model training through ensuring data quality, using different datasets for training, testing and validation, and the periodic reviewing and updating of datasets.

For more information on the Model AI Framework, please refer to the “Board of directors/governance” section. The IMDA has also embarked on a study (in partnership with nine countries) to test LLMs for bias stereotypes across different cultures.⁴⁹

National security and military

The Ministry of Defence (“MINDEF”) and the Singapore Armed Forces have been harnessing AIDA to enhance servicemen’s safety during training sessions and field operations.⁵⁰ Examples include the fielding of unmanned ground vehicles for logistics support, deploying automatic detection and classification of runway damage with the use of drones, deploying coastal security systems equipped with advanced video analytics and employing detection analytics to hunt cyber threats.⁵¹

Singapore, like many other countries, must also navigate both multilateral and unilateral export control regimes when it comes to the high-performance computing resources (i.e. GPUs) for AI model training and inference. While Singapore is not legally obliged to enforce the unilateral export control measures of other countries, the Singapore Government has stated that all companies operating in Singapore must take into account such export control measures that apply to their international business activities, and must conduct their business transparently.⁵² The Singapore Government will take the necessary enforcement action if Singapore laws have been breached (e.g. false declarations are made to Singapore authorities).

Conclusion

Singapore continues to support the use of AI with funding, training and guidance from regulators. With growing international interest in this area as more countries release guidelines, hold public consultations and even introduce legislation regulating the use of AI, Singapore continues to monitor developments around the world to harness the most effective uses of the technology, in a way that maximises its benefits and minimises the risk of harm to any person.



Endnotes

- 1 The IMDA, *Services and Digital Economy Technology Roadmap* (last accessed 19 February 2025), <https://www.imda.gov.sg/about-imda/research-and-statistics/sgdigital/services-and-digital-economy-technology-roadmap>
- 2 Smart Nation Singapore, *National Artificial Intelligence Strategy* (19 November 2019), <https://www.smartnation.gov.sg/files/publications/national-ai-strategy.pdf>
- 3 Smart Nation Singapore, *National Artificial Intelligence Strategy 2.0*, <https://file.go.gov.sg/nais2023.pdf>
- 4 Ministry of Finance, *Budget 2025 Statement by the Prime Minister and Minister for Finance* (18 February 2025), https://www.mof.gov.sg/docs/librariesprovider3/budget2025/download/pdf/fy2025_budget_statement.pdf
- 5 The IMDA, *Singapore launches AI Verify Foundation to shape the future of international AI standards through collaboration* (7 June 2023), <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/singapore-launches-ai-verify-foundation-to-shape-the-future-of-international-ai-standards-through-collaboration>
- 6 For example, through white papers detailing assessment methodologies and the open-source toolkit released by the Veritas Consortium.
- 7 For instance, Singapore has signed Memoranda of Understanding with the Republic of Korea and Australia to cooperate on AI research.
- 8 The Ministry of Communications and Information, *Singapore and the US to deepen cooperation in AI* (13 October 2023), <https://www.mci.gov.sg/media-centre/press-releases/singapore-and-the-us-to-deepen-cooperation-in-ai>

- 9 The IMDA, *New crosswalk with ISO/IEC 42001: 2023 shows international alignment* (June 2024), <https://aiverifyfoundation.sg/resources>, with the crosswalk document available at <https://aiverifyfoundation.sg/wp-content/uploads/2024/06/Crosswalk-AIV-and-ISO42001-final.pdf>
- 10 The ASEAN Secretariat, *ASEAN Guide on AI Governance and Ethics*, <https://asean.org/book/asean-guide-on-ai-governance-and-ethics>
- 11 The ASEAN Secretariat, *Expanded ASEAN Guide on AI Governance and Ethics – Generative AI*, <https://asean.org/book/expanded-asean-guide-on-ai-governance-and-ethics-generative-ai>
- 12 The IMDA, *AI Playbook for Small States* (22 September 2024), <https://www.imda.gov.sg/-/media/imda/files/news-and-events/media-room/media-releases/2024/09/ai-playbook-for-small-states/imda-ai-playbook-for-small-states.pdf>
- 13 The Supreme Court of Singapore, *Guide on the Use of Generative Artificial Intelligence Tools by Court Users* (23 September 2024), https://www.judiciary.gov.sg/docs/default-source/circulars/2024/registrar's_circular_no_1_2024_supreme_court.pdf?sfvrsn=996ec0d1_1
- 14 The IPOS, *When Code Creates: Landscape Report on IP Issues in AI*, <https://isomer-user-content.by.gov.sg/61/4f89205f-3320-4d34-9466-a85a87ebc0a4/when-code-creates-landscape-report-on-ip-issues-in-ai.pdf>
- 15 For example, using the method in controlling the navigation of an autonomous vehicle.
- 16 Channel News Asia, *As ChatGPT Takes the World by Storm, Professionals Call for Regulations and Defences against Cybercrime* (16 February 2023), <https://www.channelnewsasia.com/singapore/chatgpt-ai-chatbot-risks-regulations-cybercrime-phishing-3282896>
- 17 *Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd* [2011] 4SLR 381 at [41], [72].
- 18 *Ibid.* at [81].
- 19 *Ibid.* at [75].
- 20 Section 34 of the Competition Act.
- 21 Section 47 of the Competition Act.
- 22 Section 54 of the Competition Act.
- 23 The CCCS (in collaboration with the IPOS and the PDPC), *Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights* (2 December 2020); the PDPC (in collaboration with the CCCS), *Discussion Paper on Data Portability* (25 February 2019).
- 24 The CCCS, *Data: Engine for Growth – Implications for Competition Law, Personal Data Protection, and Intellectual Property Rights* (2 December 2020).
- 25 *Ibid.* at pages 66 to 68.
- 26 The CCCS (in an interview with MLex), *Comment: AI is both a concern and a tool for Singapore's competition regulator* (13 September 2024), <https://www.ccs.gov.sg/-/media/custom/ccs/files/media-and-publications/publications/journal/mlcxcomment-ai-is-both-a-concern-and-a-tool-for-singapores-competition-regulator.ashx>
- 27 Other concerns relate to how an organisation's independent and rational business justifications for using a third-party pricing algorithm may be weighed against any anti-competitive effect that may result from such use, and how liability may be established for any autonomous decision-making that results in collusive outcomes in situations involving self-learning algorithms.
- 28 The Model AI Framework was recognised by a top award in the "Ethical Dimensions of the Information Society" category by the World Summit on the Information Society Prizes.
- 29 The IMDA, *Invitation to Pilot: AI Verify – AI Governance Testing Framework & Toolkit* (25 May 2022), <https://file.go.gov.sg/aiverify.pdf>
- 30 The IMDA, *Singapore launches AI Verify Foundation to shape the future of international AI standards through collaboration* (7 June 2023), <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/singapore-launches-ai-verify-foundation-to-shape-the-future-of-international-ai-standards-through-collaboration>

- 31 The IMDA, *Singapore proposes framework to foster trusted Generative AI development* (16 January 2024), <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/public-consult-model-ai-governance-framework-genai>
- 32 Section 13 of the PDPA.
- 33 The PDPC, *Advisory Guidelines on the PDPA for Selected Topics* (revised 17 May 2022), at [3.35].
- 34 The PDPC, *Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems* (issued 1 March 2024), at [7.8] to [7.12].
- 35 Part 5 of the Cybersecurity Act 2018.
- 36 The CSA, *Guidelines and Companion Guide on Securing AI Systems* (15 October 2024), <https://www.csa.gov.sg/resources/publications/guidelines-and-companion-guide-on-securing-ai-systems>
- 37 Section 2(1) of the Road Traffic Act 1961.
- 38 Rule 9 of the Autonomous Vehicles Rules.
- 39 The AI Verify Foundation, *Generative AI: Implications for Trust and Governance* (5 June 2023), https://aiverifyfoundation.sg/downloads/Discussion_Paper.pdf
- 40 The AI Verify Foundation, *Cataloguing LLM Evaluations* (31 October 2023), https://aiverifyfoundation.sg/downloads/Cataloguing_LLM_Evaluations.pdf
- 41 The IMDA, *First of its kind Generative AI Evaluation Sandbox for Trusted AI by AI Verify Foundation and IMDA* (31 October 2023), <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/generative-ai-evaluation-sandbox>
- 42 The AI Verify Foundation, *Model AI Governance Framework for Generative AI* (30 May 2024), <https://aiverifyfoundation.sg/resources/mgf-gen-ai>
- 43 The MAS, *MAS Partners Industry to Develop Generative AI Risk Framework for the Financial Sector* (15 November 2023), <https://www.mas.gov.sg/news/media-releases/2023/mas-partners-industry-to-develop-generative-ai-risk-framework-for-the-financial-sector>
- 44 The MAS, *Emerging Risks and Opportunities of Generative AI for Banks*, <https://www.mas.gov.sg/-/media/mas-media-library/schemes-and-initiatives/ftig/project-mindforge/emerging-risks-and-opportunities-of-generative-ai-for-banks.pdf>
- 45 Channel News Asia, *Generative AI being tested for use in Singapore Courts, starting with small claims tribunal* (27 Sep 2023), <https://www.channelnewsasia.com/singapore/artificial-intelligence-court-small-claims-singapore-chatgpt-3801756>
- 46 See for instance The Straits Times, *NEA exploring table-cleaning robot at hawker centres to support manual labour* (28 November 2022), <https://www.straitstimes.com/singapore/environment/nea-exploring-table-cleaning-robot-at-hawker-centres-to-support-manual-labour>; Channel News Asia, *Local cleaning robotics firms see demand at least double amid tech advances* (19 April 2022), <https://www.channelnewsasia.com/watch/local-cleaning-robotics-firms-see-demand-least-double-amid-tech-advances-video-2634181>; and The Straits Times, *Autonomous cleaning bot to start scrubbing public toilets in early 2024* (4 December 2023), <https://www.straitstimes.com/tech/autonomous-cleaning-bot-to-start-scrubbing-public-toilets-in-early-2024>
- 47 Enterprise Singapore, *Enterprise Development Grant* (last accessed 20 February 2025), <https://www.enterprisesg.gov.sg/financial-support/enterprise-development-grant>
- 48 The IMDA, *A Guide to Job Redesign in the Age of AI* (4 December 2020).
- 49 The IMDA, *Singapore AI Safety Red Teaming Challenge: Evaluation Report* (11 February 2025), <https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/singapore-ai-safety-red-teaming-challenge-evaluation-report.pdf>
- 50 The MINDEF, *Fact Sheet: Leveraging Digital Technology and Research to Enhance Safety of National Servicemen* (3 March 2022), https://www.mindef.gov.sg/news-and-events/latest-releases/03mar22_fs2
- 51 The MINDEF, *Speech by Senior Minister of State for Defence, Mr Heng Chee How, for Joint Grant Awards Ceremony of the Robust AI and AI for Materials Discovery Grand Challenges on 26 July 2023* (26 July 2023), https://www.mindef.gov.sg/news-and-events/latest-releases/26jul23_speech

- 52 The Ministry of Home Affairs, *Transcript of Media Conference With Mr K Shanmugam, Minister for Home Affairs and Minister for Law, Regarding the Case Involving the Three Men Who Were Charged on 27 February 2025 for Fraud by False Representation* (3 March 2025) <https://www.mha.gov.sg/mediaroom/speeches/transcript-of-media-conference-with-mr-k-shanmugam-minister-for-home-affairs-and-minister-for-law-regarding-the-case-involving-the-three-men-who-were-charged-on-27-february-2025-for-fraud-by-false-representation>; The Ministry of Foreign Affairs, *Minister for Foreign Affairs Dr Vivian Balakrishnan's Oral Reply to Supplementary Question on Singapore's Role as an International Trading Hub* (18 February 2025), <https://www.mfa.gov.sg/Newsroom/Press-Statements-Transcripts-and-Photos/2025/02/Oral-reply-to-SQ>



Lim Chong Kin

Tel: +65 6531 4110 / Email: chongkin.lim@drewnapier.com

Chong Kin is the Managing Director of Drew & Napier's Corporate & Finance Department and heads the Telecommunications, Media and Technology ("TMT") Practice. He also co-heads the Data Protection, Privacy & Cybersecurity Practice, as well as the Competition Law & Regulatory Practice.

Chong Kin played a key role in the liberalisation of the telecommunications, media and postal industries in Singapore. Since 1999, he routinely advises the sectoral regulators on liberalisation, market access, licensing, competition regulation, merger reviews and enforcement issues, including successfully defending the regulators in many Ministerial appeals. He was an early pioneer in the practice of competition laws in Singapore, through drafting of the competition frameworks that continue to govern the telecoms, media and postal sectors today. Chong Kin is also a pioneer in the practice of data protection, being relied upon by Singapore's data protection commission to draft their implementation guidelines, assist in complex enforcement of data breach cases, and develop cross-border frameworks.



Anastasia Su-Anne Chen

Tel: +65 6531 4123 / Email: anastasia.chen@drewnapier.com

Anastasia is a Director with the Corporate & Finance Department in Drew & Napier. Her key areas of practice are TMT, data protection and cybersecurity. She was formerly the Deputy Chief Counsel of the Personal Data Protection Commission ("PDPC") and Infocomm Media Development Authority ("IMDA") for over nine years, where she was the lead counsel for PDPC's matters, IMDA's procurement and Intellectual Property portfolios, as well as the legal advisor to IMDA's Data Administration Group.

Anastasia has extensive experience advising on TMT and data protection-related matters from both the public and private sector perspectives. Data protection matters include data protection compliance programmes, data transfer agreements, privacy notices, data retention schedules, outsourcing of data processing and impact assessments.



Cheryl Seah


Tel: +65 6531 4167 / Email: cheryl.seah@drewnapier.com

Cheryl is a Director with the Corporate & Finance Department in Drew & Napier. Her key areas of practice are TMT and administrative and public law. Cheryl advises clients on regulatory matters, ranging from cybersecurity to payment services to gaming. She also advises companies ranging from Fortune 500 MNCs to start-ups on legal, contractual and governance issues arising from their use of AI: from procuring the high-performance computing resources (i.e. GPUs), to the data used in model training, to the IP and liability issues arising from the output. Clients include legal technology providers deploying their products in Singapore, and companies who wish to customise their own generative AI applications to generate documents and code.

Drew & Napier LLC

10 Collyer Quay, 10th Floor Ocean Financial Centre, Singapore 049315

Tel: +65 6531 4110 / URL: www.drewnapier.com



Global Legal Insights – AI, Machine Learning & Big Data provides analysis, insight and intelligence across 22 jurisdictions, covering:

- Trends
- Ownership/protection
- Antitrust/competition laws
- Board of directors/governance
- Regulations/government intervention
- Generative AI/foundation models
- AI in the workplace
- Implementation of AI/big data/machine learning into businesses
- Civil liability
- Criminal issues
- Discrimination and bias
- National security and military

globallegalinsights.com