# CNPLAW TECHNOLOGY SERIES: THE RISE OF AI, BIG DATA AND MACHINE LEARNING

*Posted on September 25, 2023*

**Category:** CNPupdates

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.

**Authors: Wong Pei-Ling and Ong Hong Yi**

## Introduction:

In recent years, the world has witnessed a remarkable surge in the development and deployment of artificial intelligence ("**AI**") technologies, big data, and machine learning across various industries. AI leverages on computers and machines to mimic the problem-solving and decision-making capabilities of the human mind. In the healthcare sector, big data has assisted scientists in developing precision medicine in public health and aided in the development of technology enabling genome editing. In the retail sector, consumers source for the cheapest flight tickets through flight scanner applications using big data. Retailers have successfully used big data to personalise advertisements targeting specific groups of consumers who exhibit certain identified behavioural patterns through their online activity. In the finance sector, insurance companies utilize big data on driving history to assess insurance premiums with greater accuracy. Employers leverage on big data to determine the most suitable candidates to hire or fire. Ultimately, proper use of big data will allow for more accurate decision-making, leading to greater opportunities for innovation and efficiency.

As the proliferation of AI, big data, and machine learning steadily infiltrates every facet of our daily lives, it is important for individuals, organisations, and regulatory bodies to understand the benefits and potential risks associated with its use. Whilst AI holds tremendous potential to enhance productivity and improve decision-making, its use may also give rise to ethical, legal, and societal dilemmas, when not handled with sufficient care and know-how, demanding a delicate balance between progress and responsibility.

The urgency of ensuring the responsible use of AI can already be observed in the United States – European Union Joint Statement of the Trade and Technology Council, which stipulates that a draft voluntary code of conduct on AI will be prepared to "reaffirm their commitment to a risk-based approach to AI to advance trustworthy and responsible AI technologies."

In the local context, this article serves to highlight some of the initiatives, frameworks and regulations available in Singapore, and the legal obligations arising from the use of AI, big data and machine learning.

## Initiatives/frameworks and regulations

The Smart Nation Initiative was launched in 2014 in response to the Government's plans to transform Singapore into a smart nation by the adoption and use of AI, big data and machine learning. AI Singapore, a national AI programme set up by the National Research Foundation, was subsequently launched in 2017 to bring together Singapore-based research institutions, AI start-ups and companies tasked with developing AI products within a vibrant ecosystem that will enable use-inspired research, encourage knowledge growth, tool creation and the development of talent to power Singapore's AI efforts. Other initiatives or frameworks that were launched include the Smart National and Digital Government Office ("**SNDGO**") and

General disclaimer
This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.

SGInnovate, a Government-owned company that invests in Deep Technology start-ups in Singapore, under the National Research Foundation.

One of the key issues arising from the use of AI, big data, and machine learning would be the collection, use and disclosure of personal data. In this regard, the Personal Data Protection Act recognises that there are exceptions to the need for consent for the collection and use of personal data. Such exceptions include personal data that is collected and used to further the legitimate interests of *inter alia*, the organisation and where its collection and/or use is intended for business improvement purposes, such as to improve, enhance or develop new products for the organisation. Both exceptions are subject to certain conditions (for example, under the legitimate interest exception, the organisation must show that such legitimate interests outweigh any adverse effects on the individual whose personal data is collected for use by the organisation).

To this end, the Personal Data Protection Commission ("**PDPC**") has introduced a Model AI Governance Framework in 2020 to provide guidance and recommendations to organisations, enabling them to implement the use of AI in a responsible manner. While the adoption of the recommendations from the Model AI Governance Framework is purely voluntary, organisations are strongly encouraged to do so as their collective efforts would promote the use of AI responsibly. The Model AI Governance Framework focuses on four broad areas:

- <u>Internal governance structures and measures:</u> Organisations should adapt existing or set up internal governance structure(s) and measures to incorporate values, risks and responsibilities relating to algorithmic decision-making;
- <u>Determining the level of human involvement in AI-augmented decision making:</u> Organisations may refer to a methodology aimed at aiding and setting its risk appetite for the use of AI, i.e. determining acceptable risks and identifying an appropriate level of human involvement in AI-augmented decision-making;
- <u>Operations management:</u> Organisations should consider data and quality management, including the development, selection and maintenance of AI models; and
- <u>Stakeholder interaction and communication:</u> Organisations should put in place strategies for communication and managing relationships with stakeholders.

The Model AI Governance Framework and the Implementation and Self-Assessment Guide for Organisations will enable organisations to assess their internal processes with a view towards promoting the use of AI in a safe and responsible manner. Further to this, the PDPC has also published a Compendium of Use Cases (Volume 1 and 2) to demonstrate how local and international organisations of varying scale implement and/or align their AI governance processes with the Model AI Governance Framework. The Implementation and Self-Assessment Guide for Organisations, when used together with the Compendium of Use Cases, are intended to assist organisations to (i) better identify potential and existing risks in their internal processes and (ii) take steps to address them.

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.

While it is important that organisations do their part to ensure that potential and existing risks arising from the implementation of AI are managed responsibly through an examination of their internal processes, the general public need to be assured that AI systems used by organisations are fair, explainable and safe, and that organisations that deploy them are transparent and accountable. To this end, the PDPC, together with the Infocom Media Development Authority ("IMDA"), have developed A.I. Verify, an AI Governance Testing Framework and Toolkit, which will enable the IT industry in Singapore to demonstrate that their deployment of AI is undertaken responsibly. This is currently available as a Minimum Viable Product (MVP) for system developers and owners who want to be more transparent on the performance of their AI systems, through a combination of technical tests and process checks.  The IMDA is currently inviting participants from the broader IT industry (i.e. (i) AI system owners and developers who wish to verify that their AI systems meet internationally accepted AI ethics and principles; (ii) technology solution providers who wish to contribute towards the development of AI governance, implementation and testing; and (iii) other testing framework owners and developers who wish to have early discussions on compatibility and interoperability) to participate in this pilot phase of the MVP.

In some cases, the use of AI technology may introduce risks of unintended discrimination potentially leading to unfair outcomes (for example, the use of AI in the automatic selection of schools based on information submitted into a system) and ethical issues when AI is tasked with making significant or sensitive decisions for consumers, taking away their free choice. For example, AI technology may use stored medical or drug purchase information for the marketing of other new medical devices or products that the patient may not necessarily require. Global positioning system ("**GPS**") or navigation mapping software programmes that provide positioning and navigation tracking services may store a user's daily routes for ease of retrieval but this may infringe on the user's rights to privacy and subject the user to targeted security risks, if the data falls into the wrong hands.

In some cases, organisations may engage third-party service providers ("**Data Intermediary**") to process data, including personal data on their behalf. Where organisations engage a Data Intermediary to process personal data on their behalf, they should understand the risks involved in the outsourcing of such data processing. Under the Personal Data Protection Act, organisations remain ultimately responsible for the personal data processed on their behalf by a Data Intermediary. The PDPC recommends that organisations regularly identify and assess potential risks pertaining to personal data breaches and establish protective measures against such breaches. When assessing a potential Data Intermediary who will process personal data on their behalf, organisations should ensure that the Data Intermediary has in place processes that will satisfy all of the obligations under the Personal Data Protection Act, including having in place reasonable security arrangements to protect the personal data in its care, and to prevent their unauthorised access, collection, use or disclosure. This can be achieved by robust due diligence enquiries, and carefully considering the Data Intermediary's data protection policies, internal training programs, security measures and relevant certifications. By extension, it would also be crucial for organisations to set out the scope of the data processing activities that are to be undertaken by the Data Intermediary, and a separate data sharing contract should be entered into between the parties which *inter alia* include terms on the transfer and storage of personal data.

The Personal Data Protection Act allows for personal data which has been anonymised to be used by organisations for research, data analytics and machine learning. However, technologies have advanced such that structured, textual and non-complex data may now be de-anonymised to identify individuals by drawing inferences on otherwise anonymised personal identifiers and the attributes of individuals from personal data that was previously anonymised. In this regard, the PDPC has published a Guide to Basic Anonymisation which sets out recommended steps and techniques to reduce the risk of de-anonymisation and re-identification.

Amendments have also been made to the Copyright Act in November 2021, to permit the use of copyrighted materials for "computational data analysis". Such materials may be text-based works, sounds or images, provided that the user is lawfully entitled to access and use the materials, and subject to the satisfaction of certain conditions. The user is not permitted to supply a copy of the works to any person other than for the purpose of verifying the results of the computational data analysis carried out by the user or collaborative research or study relating to the computational data analysis.

Nonetheless, the Copyright Act is silent when it comes to determining the author of an AI generated work. At present, only natural persons may be considered authors of authorial works. In this regard, the Copyright Act arguably affords scant protection to AI generated works given that copyright protection subsists only in an authorial work, including *inter alia* that the author is a "qualified individual" (which points to the author being a natural person). The Singapore Court of Appeal in *Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd* (2011) 4 SLR 381 took the view that copyright protection will only arise where the work was created by a human author. The Singapore Court of Appeal in *Global Yellow Pages Ltd v Promedia Directories Pte Ltd*  2 SLR 185, affirmed that for copyright protection to subsist in a literary work, there must be an "*authorial creation*" that is "*causally connected with the engagement of the human intellect*". *By the human intellect, we mean the application of intellectual effort, creativity or the exercise of mental labour, skill or judgment.*" Given that AI generated works are simply works or end-products generated by the use of AI and, arguably, not by a natural person, it remains to be seen as to how such works may be characterised and ruled by the Courts to be an authorial creation of the human intellect in the event of a copyright dispute.

In a bid to prepare for the use of autonomous vehicles on the roads in the near future and to facilitate trials for their use, The Road Traffic Act was amended to introduce a definition of "autonomous motor vehicle" which means "a motor vehicle equipped wholly or substantially with an autonomous system *also commonly known as a driverless vehicle, and includes a trailer drawn by such a motor vehicle". It is interesting to note that A*Star's self-driving vehicle was first approved for public road testing as far back as July 2015. The National University of Singapore ("**NUS**") and the Singapore-MIT Alliance for Research and Technology ("**SMART**") have also collaborated to design autonomous research prototype cars around the NUS campus, where riders can book and select their desired pick-up and drop-off locations using their smartphones, much like an on-demand shuttle service. The term "autonomous system" for a motor vehicle, means “a system that enables the operation of the motor vehicle without the active physical control of, or monitoring by, a human operator” and the term “automated vehicle technology” has been defined to mean “any particular technology that relates to the design, construction or use of autonomous motor vehicles; or otherwise relates to advances in the design or construction of autonomous motor vehicles”. Parties who are interested may also note that Enterprise Singapore has published a set of standards, titled Technical Reference 68, which sets out the standards expected to be complied with respect to basic behaviour, safety, cybersecurity and vehicular data types and formats.

## Civil and Criminal Liability in respect of AI, big data and machine learning

One of the hotly debated issues in the technology space pertains to the use of generative AI chatbot programmes that simulate human conversations with the aim to provide users (i.e. customers) with better products and services.  While some of the generative AI chatbots such as Siri and Alexa have been around for a while with less hype, the more recently launched large language models (“**LLMs**”) such as ChatGPT and Bard have sparked an AI arms race between the technology giants, and users are now grappling with issues ranging from ethical and responsible usage, to concerns over heightened cybersecurity risks.

These generative AI chatbot programmes share a common theme in that they collect a vast amount of data from various internet resources, including millions of online books, articles, websites and the social media, and are “pre-trained” on huge amounts of image or text data to predict the next word in a sequence and have the ability to generate responses to queries from users, simulating conversations with an intelligent being. These AI chatbot programmes may also generate essays and articles with an impressive degree of accuracy, and write poetry using certain key words, although some users have cited that there are limitations as to accuracy and biasness, depending on the subject matter. We understand that this may be inevitable as the training data collected may reflect the opinions of certain groups as the programmes work on a combination of deep learning algorithms and natural language processing. On the positive side, these AI chatbot programmes may be used in conjunction with other communication apps, such as Microsoft Teams and Skype to enhance productivity.

The widespread use of AI, big data, and machine learning makes it difficult to imagine having an all-encompassing piece of legislation or directive that will adequately deal with advanced technological disruptions and their potential for misuse or abuse. Currently, any misuse or abuse of AI, big data and machine learning are dealt with by individual pieces of legislation in Singapore.

Technological advances mean that it is now easier than ever before to employ the use of AI to spread misinformation and affect national security, public health, safety and other interests. In this regard, the Protection from Online Falsehoods and Manipulation Act renders it an offence for a person, whether in or outside Singapore, to make or alter a bot with the intention of communicating or enabling any other person to communicate, by means of the bot, a false statement of fact in Singapore.

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.

In the context of cryptocurrencies, the Singapore International Commercial Court in *B2C2 Ltd v Quoine Pte Ltd* 4 SLR 17 ruled that when knowledge had to be ascertained in the context of deterministic systems (meaning systems that are not autonomous and require input in a pre-ordained manner) as opposed to fully autonomous systems, the assessment of such knowledge shall be made with reference to the programmer at the time the programme was written, and not the time that the smart contract was entered into. This decision was made against the backdrop of an earlier technical glitch on Quoine's cryptocurrency platform which had caused B2C2 to initiate trades at a rate that was approximately 250 times the then market rate in favour of B2C2, resulting in Quoine unilaterally cancelling those trades giving rise to the dispute. However, it remains unclear as to how Singapore courts would deal with fully autonomous systems having "a mind of its own".

The use of AI, big data, and machine learning may constitute computer material or services which may be covered by the Computer Misuse Act. The term "Computer" has been defined to mean an "electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices" with certain other exclusions falling out of this definition. In this regard, the Computer Misuse Act imposes criminal liability on certain prohibited activities such as hacking, identity theft/fraud, denial of service attacks, infection of information technology systems with malware and the possession, use, distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime.

## Conclusion

Despite the challenges faced in implementing laws that are sufficiently robust to keep up with the rapid changes in the development of AI, big data, and multi-faceted machine learning capabilities, varying degrees of success have been observed.

In the area of personal data regulation, the Personal Data Protection Act sets out clearly the obligations of an organisation and its Data Intermediary. The Ministry of Communications and Information has announced its plans to issue Advisory Guidelines on the Use of Personal Data in AI Systems under the Personal Data Protection Act within the year. In the area of copyright law, further development in case law may be necessary to provide clarity on whether copyright subsists in AI generated works. While the publication of Technical Reference 68 alongside recent amendments to the Road Traffic Act have contemplated the introduction of autonomous vehicles, there is no clear guidance on related issues such as the interface between an autonomous vehicle and its passengers.

In other areas of AI deployment, the context in which the law provides adequate protection is arguably narrow. The communication of false statements of fact through the use of a bot is an offence under the Protection from Online Falsehoods and Manipulation Act, knowledge can be ascertained with reference to the programmer at the time of programming in the context of deterministic systems, and the commission of

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.

cybercrime through AI systems may be dealt with under the Computer Misuse Act.

AI Singapore, <https://aisingapore.org/>.

Personal Data Protection Act 2012.

Personal Data Protection Act 2012.

Personal Data Protection Commission, "Guide to Managing Data Intermediaries".

Personal Data Protection Act 2012.

Personal Data Protection Act 2012.

Personal Data Protection Commission, "Guide to Basic Anonymisation".

Copyright Act 2021.

Copyright Act 2021.

Copyright Act 2021.

Section 77 Copyright Act 2021.

*Asia Pacific Publishing Pte Ltd v Pioneers & Leaders (Publishers) Pte Ltd* (2011) 4 SLR 381.

*Global Yellow Pages Ltd v Promedia Directories Pte Ltd* 2 SLR 185.

Road Traffic Act 1961.

Section 2 Road Traffic Act 1961.

Section 2 Road Traffic Act 1961.

Section 2 Road Traffic Act 1961.

CETRAN, "Singapore Publishes Technical Reference for AVS".

Protection from Online Falsehoods and Manipulation Act 2019.

Section 8 Protection from Online Falsehoods and Manipulation Act 2019.

B2C2 Ltd v Quoine Pte Ltd 4 SLR 17.

Computer Misuse Act 1993.

Section 2 Computer Misuse Act 1993.

Computer Misuse Act 1993.

Sections 3 – 10 Computer Misuse Act 1993.

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.

Personal Data Protection Act 2012.

Road Traffic Act 1961.

Protection from Online Falsehoods and Manipulation Act 2019.

B2C2 Ltd v Quoine Pte Ltd 4 SLR 17.

Computer Misuse Act 1993.

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.