SINGAPORE ACADEMY OF LAW CONSIDERS THE IMPACT OF ROBOTICS AND ARTIFICIAL INTELLIGENCE ON THE LAW

Date: 4 March 2021

Singapore Artificial Intelligence Alert

By: Lucas Nicolet-Serra, Daniel Knight

This publication is issued by K&L Gates in conjunction with K&L Gates Straits Law LLC, a Singapore law firm with full Singapore law and representation capacity, and to whom any Singapore law queries should be addressed. K&L Gates Straits Law is the Singapore office of K&L Gates, a fully integrated global law firm with lawyers located on five continents.

The Law Reform Committee (LRC) of the Singapore Academy of Law (SAL) established a Subcommittee on Robotics and Artificial Intelligence to consider and make recommendations regarding the application of the law to AI systems. The LRC is considering whether existing systems of law, regulation, and wider public policy remain "fit for purpose," given the pace and ceaselessness of change of the AI field. The LRC published two reports in July 2020, one report in September 2020, and one report in February 2021:

- "Applying Ethical Principles for Artificial Intelligence in Regulatory Reform";
- "Rethinking Database Rights and Data Ownership in an AI World";
- "Report on the Attribution of Civil Liability for Accidents Involving Autonomous Cars"; and
- "Report on Criminal Liability, Robotics and AI Systems."

This initiative is part of the report series on "impact of robotics and artificial intelligence on the law" to stimulate systematic thought and debate on these issues and discussions between policy makers, legislators, industry, the legal profession, and the public to adopt legislation in line with the evolution of AI. The remaining two reports of the series cover application of criminal law to the operation of AI systems and technologies, and attribution of civil liability for accidents involving automated cars.

This article examines each report and highlights issues currently under consideration that may impact industries in Singapore whose business models, operations, or products may rely on AI systems and/or robotics.

REPORT 1: APPLYING ETHICAL PRINCIPLES FOR ARTIFICIAL INTELLIGENCE IN REGULATORY REFORM

Report 1 by the Subcommittee identifies issues that law and policy makers may face in applying ethical principles when developing or reforming policies and laws regarding AI. The primary objective of this report is to advance a public discussion about how those ethical principles can be incorporated into the development of "fair, just,

appropriate and consistent laws, regulations and 'soft law' measures that foster technological development that prioritises human wellbeing and promotes human dignity and autonomy." Specifically, the report discusses the following ethical principles that should be relevant for legal reform for AI:

Law and Fundamental Interests

AI systems should be designed and deployed to comply with law and not violate established fundamental interests of persons protected by law — the two main issues with regard to liability of AI systems are the (i) lack of mental state of the relevant actor such as knowledge or intention attributable to a person and (ii) a "decision" by an AI system to act is the result of a long causation chain involving different actors at different stages of the system's creation and deployment.

Considering AI Systems' Effects

Designers and deployers of AI systems should consider the likely effects of reasonably foreseeable effects of AI systems throughout their lifecycle. It is possible that existing principles are sufficient and could be relied upon to fairly apportion liability. However, policy makers may require more tailor-made interventions by creating principles specific to certain scenarios.

Wellbeing and Safety

AI systems should be rational, fair, and without intentional or unintentional biases. It is necessary to assess AI systems' intended and unintended effects against holistic wellbeing and safety metrics and minimize harm by considering factors such as human emotions, empathy, and personal privacy.

Risk Management to Human Wellbeing

It is imperative for designers and deployers of AI systems to properly assess and eliminate or control risks of the use of AI systems as a matter of safety and wellbeing. Policymakers will need to consider whether mandatory risk management standards need to be imposed, and if so, the form in which, and specificity with which, such standards are articulated.

Respect for Values and Culture

AI systems should be designed to take into account, as far as reasonably possible, societal values and cultural diversity and values in different societies in AI deployment. Taking into account societal values and cultural norms is especially important in effective AI systems.

Transparency

Designing AI systems to be transparent as far as reasonably possible and to enable discovery of how and why an AI system made a particular decision or acted the way it did. Transparency entails being able to trace, explain, verify, and interpret all aspects of AI systems and their outcomes insofar possible. The objective is to not only properly regulate AI but also to build trustworthy AI. One possible regulatory response to challenges involving tracing, explaining, and verifying different aspects of AI is to require mechanisms to be built into AI systems that, as far as reasonably possible, record input data and provide a logic behind decisions taken by the AI, very much like a plane black-box recorder.

Accountability

Holding appropriate persons accountable for the proper functioning of AI systems based on their roles, the context, and consistency with the state of art.

Ethical Data Use

Good privacy and personal data management practices to protect the personal data of individuals.

REPORT 2: RETHINKING DATABASE RIGHTS AND DATA OWNERSHIP IN AN AI WORLD

Report 2 by the Subcommittee identifies key data-related and intellectual property laws on databases and data ownership, especially those that relate to “big data” databases used for AI systems. Any deficiencies in laws on data or databases may have ripple effects on laws managing AI systems.

Databases

Existing Legal Protections

The Subcommittee analyses whether the protection of databases under copyright and patent law is adequate. Current protection in Singapore is limited to elements that meet the requisite level of originality (i.e., application of intellectual effort, creativity, or the exercise of a mental labor, skill, or judgment). In contrast, big data compilations do not have a single author; rather, they consist of automated data collected into raw machine-generated databases. The focus on the creative element excludes from protection valuable databases.

Recommendations

Introduction of a sui generis database right[1] is not appropriate under Singapore law given the limited evidence of its effectiveness. The Subcommittee recommends that (i) copyright protection of computer-generated works be recognized and (ii) greater clarity as to how compilation rights apply for the copyright protection and how records of authorship of databases can be properly maintained.

Data Ownership

Current Status

The report reviews whether data collected by AI, whether as individual data or a combination of data elements, need to be granted property rights. Personal data is protected in Singapore under the Personal Data Protection Act (PDPA), but even if the data subject enjoys certain protection, he/she is not granted legal ownership of his/her data. Given the nature of data, there are fundamental difficulties—on grounds of jurisprudential principle and policy—to using ownership and property rights as legal frameworks to control data.

Merits of Granting Property Rights Over Personal Data

There are various arguments for granting property rights over data, such as providing a clear and coherent method to protect privacy and relying on existing property laws to provide established protection. Currently, data is protected through a mix of copyright, confidentiality, and privacy laws.

Recommendations

The report concludes that creating a property right for data is not desirable due to the conceptual challenges of data's intangibility. Introducing particular rights or entitlement over personal data can be achieved by other means

than ownership (e.g., data portability obligation under the PDPA). Specific data control methods can be implemented to protect individual rights as well as to support data innovation.

REPORT 3: ATTRIBUTION OF CIVIL LIABILITY FOR ACCIDENTS INVOLVING AUTONOMOUS CARS

Under consideration by regulators are questions regarding the attribution of civil liability when accidents or collisions involving autonomous cars occur and cause injury or death, even though it is hoped that autonomous vehicles will significantly reduce the number of accidents on public roads.

At present (i.e., for car accidents involving human drivers), Singapore law applies a fault-based negligence framework: the person most responsible for the accident is held liable (that liability then typically being covered by motor insurance).

For self-driving cars, many events leading up to an accident may stem from decisions made by the car's autonomous features, with no human input or intervention whatsoever. As the car cannot be meaningfully held accountable and sued directly, it becomes important whether to attribute liability to either the car's manufacturer, the manufacturer of the components that did not function properly, or the car's owner or user.

Authorities in various overseas jurisdictions have taken recent steps to review and reform aspects of their laws to accommodate the arrival on public roads of, in the first instance, conditionally autonomous cars—where a human driver is still required to take back control if necessary.

To date, the approach in Singapore has been to introduce “sandbox” regulations to promote innovation in autonomous car technologies in Singapore rather than seeking to legislate now for future mainstream use. However, different liability frameworks presently used in other areas of law in Singapore (i.e., negligence, product liability, and no-fault liability) have yet to be applied to autonomous vehicles.

Negligence

Typically, negligence-based laws require the establishment of (a) a duty of care (foreseeability of harm), (b) a breach of that duty (standard of care), and (c) recoverable damage. However, failures of software present a challenge and render the question of breach much more complicated to resolve.

Product Liability

Such regime is focused on dangerous product defects and manufacturers' failure to adopt reasonable product designs that mitigate foreseeable risks of harm—such regime is well developed in Europe but is less well developed than negligence in Singapore law. In Singapore, the committee considers that strict liability is likely to have an adverse impact on the availability and cost of insurance and have a risk of stifling innovation. In addition, for Singapore, moving to a novel strict-liability regime from one based on negligence may involve significant transition costs, even if it were limited to self-driving car accidents.

No-Fault Liability

No-fault liability simply requires that if the harm was suffered due to the accident, compensation for the victim follows as a matter of course. The relative simplicity of a no-fault liability regime makes it initially attractive as a means to address the conceptual problems that self-driving cars create. However, the requirements under the

current law to prove certain legal and evidential issues should not be disregarded, and so completely abandoning them would change existing legal paradigms.

According to the committee, given Singapore's long-established negligence-based liability regime and the potential transition costs entailed in adopting a wholly new model, the more productive approach may therefore be to retain the existing system but make targeted modifications to import the desirable features of product liability and no-fault liability, where appropriate. Given this, and the fact that no other jurisdiction has yet identified a comprehensive and convincing liability framework for motor accidents involving autonomous vehicles (regardless of their level of automation), a sui generis regime may be required for Singapore.

REPORT 4: CRIMINAL LIABILITY, ROBOTICS AND AI SYSTEMS

Attribution of criminal liability to a person generally requires both a wrongful act (or, in certain cases, omission) and a mental element on the part of the person carrying out the act. That fault element, also known as “mens rea,” may involve intention, wilfulness, knowledge, rashness, or negligence.

Autonomous robotic and artificial intelligence (RAI) systems are increasingly being deployed, which can raise challenges in attributing criminal liability and holding someone responsible where harm is caused. However, while criminal liability can be imposed on natural or legal persons—and thus on both humans and corporate entities—an RAI system is not a legal person on which criminal responsibility could be placed directly.

Therefore, questions arise as to (a) which aspect of the RAI system factually caused it to act the way it did (resulting in harm), (b) which party (or parties)—be that the system manufacturer, the system owner, a component manufacturer, or a software developer—was responsible for that aspect, and (c) whether that party could have foreseen or mitigated the harm.

For RAI systems, it is useful to distinguish between cases of intentional criminal use of (or interference with) the RAI system and those where nonintentional criminal harm is caused.

For Intentional Criminal Harm

Current legislation will be applicable and could be improved but may not drastically change.

For Nonintentional Harm

In Singapore, certain offences can be satisfied when a person is criminally negligent. However, even if some existing Singapore negligence-based offences in the Penal Code could be used for RAI systems, other type of harms might not fall within the existing framework. With more complex RAI systems, it may be very difficult (in some instances, practically impossible) to establish definitively the process by which the RAI system determined to take a particular action.

Therefore, the committee has considered other mechanisms to be implemented in Singapore for RAI criminal liability:

Legal Personality of RAI Systems

One possibility that has been debated is the creation of a new form of legal personality for RAI systems, such that criminal liability could be imposed directly on the RAI system itself. However, it is unclear, for example, how imposing criminal liability and sanctions on an RAI system directly would “punish,” “deter,” or “rehabilitate” the system itself. And if the objective is instead to deter or penalize those responsible for the RAI system, that could

arguably equally be achieved through legal mechanisms that do not require new forms of legal personality to be created.

New Offences for Computer Programs

The new offences could target the creation of risk by developers or operators of computer programs through their rash or negligent creation or impose a duty on those with control over a computer program to take reasonable steps to cease harms that may result from computer programs after they manifest. This approach could allow courts to identify the persons criminally liable and the parameters of their duties. However, the contours of such offences remain uncertain, and such approach could deter innovation.

Workplace Safety Legislation as a Model

This is a model where duties are imposed on specified entities to take, so far as is reasonably practicable, such measures as are necessary to avoid harm. There is a focus on whether the relevant entity breached its statutory duty to take all reasonably practicable measures to avoid the harm. Ultimately, whether and when it is justified to place such an onus on those responsible for RAI systems is a policy judgment for lawmakers, balancing demands for accountability with the desire not to unduly stifle innovation and impede the societally beneficial development and use of RAI systems.

NEXT STEPS

K&L Gates regularly assists AI and technology companies on the implementation of innovative digital technologies. We will continue to closely monitor SAL and related government agency developments regarding the research and development of AI regulation in Singapore.

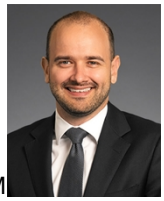
The reports of the SAL are intended to encourage systematic thought and debate between various policymaking and industry stakeholders such that public policy on AI remains close to the commercial use of AI. If you wish to get in touch with policy makers, please contact us.

FOOTNOTES

[1] Sui generis database right is a right that exists in the European Union to recognize the investment that is made in compiling a database.

KEY CONTACTS

LUCAS NICOLET-SERRA
COUNSEL
K&L GATES STRAITS LAW LLC
SINGAPORE
+65.6713.0263
LUCAS.NICOLET-SERRA@KLGATES.COM



DANIEL KNIGHT
PARTNER

MELBOURNE
+61.3.9640.4324
DANIEL.KNIGHT@KLGATES.COM

