INTRODUCTION[1]

ONG Li Min[2]
LLB (Hons) (University of Nottingham), Graduate Certificate in IP Law (Distinction), IP Academy and National University of Singapore, BBus (Hons) (Nanyang Technological University);
Research Associate, Centre for AI and Data Governance, Yong Pung How School of Law, Singapore Management University.

I. Overview of articles

1 In this special issue, we present six varied contributions from both established and emerging scholars, including those with experience in government. These contributions cover contemporary challenges in governing artificial intelligence ("AI") and data, ranging from algorithmic fairness to meta-regulation, and from local, regional and overseas viewpoints. In putting this special issue together, we sought to curate a range of topics and perspectives that would engage both legal practitioners as well as other interested readers. In this introduction, we provide an overview of the issue as a suggested guide and insert our commentary on common themes.

2 The special issue opens with "Algorithmic Fairness: Challenges and Opportunities for AI Governance" by Khoo Wu Shaun and Chow Zi En, setting the scene by emphasising the urgent need to develop rules to govern AI effectively. AI-driven technologies have been contributing to biased and unjust outcomes in society, and by exacerbating discrimination in personal realms such as healthcare, AI is proving detrimental to our social fabric. Khoo and Chow deftly lay out these issues by first defining AI technologies and then explaining the concept of algorithmic fairness. They then highlight two tensions surrounding the governance of AI: (a) mainly that fairness has conflicting definitions; and (b) how data protection objectives sit uncomfortably with the promotion of fairness

1 The research work conducted by the Guest Editor and his team was supported by the National Research Foundation, Singapore under its Emerging Areas Research Projects (EARP) Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

2 This introduction was prepared by Ong Li Min on behalf of the Guest Editor and her team members, Asst Prof Nydia Remolina Leon and Jane Loo, who worked together with her to put together this Special Issue. The author is grateful for their input; all errors remain her own. The Guest Editor and his team also thank the anonymous peer reviewers who assisted in the review of these chapters, and the Singapore Academy of Law for this editorial opportunity.

and transparency in AI. As the authors argue, "[p]roviding AI algorithms with data on the sensitive attribute enables it to take into account differential treatment and correct for it where appropriate".

3 A comparative analysis of four jurisdictions (Singapore, the EU, the US and China) was adopted, illustrating varying regulatory approaches to collecting data on sensitive attributes, addressing algorithmic fairness and applying existing anti-discrimination laws. This leads to the authors' call for deconflicting privacy regulations from AI governance (in contrast to the dominant focus on data minimisation in privacy regulations), and for recommending the articulation of fairness definitions and standards in order for AI audits to be effective. For practitioners, policymakers and researchers seeking to enter this discourse, Khoo and Chow's piece is an eye-opening and superb introduction.

4 Next, we zoom out from the assessment of algorithms to contextualising them in the digital economy. In "Cross-Border Platform Mergers in ASEAN's Digital Market", Dr Hesty Diyah Lestari looks at platform companies from a competition law angle, addressing the question: how should cross-border platform mergers in ASEAN's digital market be assessed? Practising competition lawyers would be familiar with how the 2018 merger between two major ride-hailing platforms, Grab and Uber, had generated regulatory uncertainty in the region, putting young competition agencies to task. Like Khoo and Chow, Dr Lestari adopts a comparative study to spotlight the divergent approaches to platform merger assessment and enforcement in four ASEAN Member States (*ie*, Singapore, Indonesia, the Philippines and Vietnam).

5 Dr Lestari argues that features of platform enterprises including the "multi-sidedness" of markets, network effects and (access to) big data in digital markets need to be considered in assessing whether a merger is anti-competitive. Dr Lestari calls for regional harmonisation of merger control regulations to continue attracting investment and business to the region, as well as to help achieve economic integration in ASEAN. Given the commercial realities of active mergers and acquisitions in the region, as well as its sustainable development imperatives, this is an important conversation to have.

6 The focus on digital markets segues nicely into "Artificial Intelligence and Data Governance: A Business and Human Rights Approach". In this piece, Dr Irene Pietropaoli also adopts a holistic and supranational perspective, but from a human rights angle, looking specifically at the responsibility of businesses to respect and address systemic human rights abuses in the digital economy. She criticises the overall emerging data-driven business model in the private sector and argues that business and human rights principles ought to apply.

Specifically, governments "should establish similar impact assessment requirements for businesses deploying AI systems based on the principle of human rights due diligence", stemming from the UN Guiding Principles ("UNGP"). In setting the context, Dr Pietropaoli surveyed contentious applications of AI, such as emotional AI adopted by tech companies including social media companies, illustrating the reach of AI into human thought and the challenges this poses. Dr Pietropaoli also mentions the scholarship on data colonialism and illustrates the link between people, data and AI in a commodification process.[3]

7 Dr Pietropaoli outlined the advantages of a business and human rights approach, namely that it "offers a system for the design, development and deployment of AI, and identifies responsibilities for States and businesses to address human rights impacts". She also suggests that the universality and holistic quality of such a framework could be useful, in that there exists an agreed upon standard and processes for technology impact assessments and the allocation of States' and businesses' responsibilities. In her article, Dr Pietropaoli gives a persuasive account of how the UNGP's three pillars framework – (a) state's duty to protect; (b) business responsibility to respect; and (c) access to remedy – is a ready and comprehensive framework adept for regulating the algorithmic life cycle. For instance, she argues that human rights impact assessments would bolster algorithmic accountability by assessing the full scope of impact, particularly as these would need to start with an assessment of the business model and the AI technology used. For lawyers and policymakers, the prospect of remedies under this framework is a fascinating one. Dr Pietropaoli asks us: What would access to remedy look like in the data economy? Who is to be held accountable for adverse human rights impacts caused by tech companies? These are thought-provoking and enduring questions in the larger regulatory debate.

8 This bridges over nicely to a very topical subject, *ie*, the regulation of disinformation by social media platforms, and how it would interfere with the freedom of expression. As we have seen, the proliferation of disinformation on such platforms, such as on COVID-19 vaccines, could create a climate of fear and uncertainty producing negative consequences for public health. In "Regulating Disinformation on Social Media Platforms: A Defence of the Meta-regulatory Framework", Yang Shao-Kai similarly highlights the concerns of the data-driven business model predicated on attention (platforms as "attention-brokers") and argues, as does Dr Pietropaoli, that a self-regulatory regime would not begin to address these issues. Through a power analysis (with platforms wielding

3 Dr Pietropaoli quotes Julia Powles and Hal Hodson: "Without people, there is no data. Without data, there is no AI."

"gatekeeping power") and a detailed description of the technology, Yang illustrates how platforms can amplify disinformation.

9 Yang, however, offers a different solution: meta-regulation. While profit-making motives can exacerbate the problem, he observes that platforms recognise that safe and attractive digital environments are necessary for profit generation. Further, resources and capacity reside within platforms to minimise the circulation of disinformation. As the regulatory design problem is one of incentivisation, Yang argues that meta-regulation would be most ideal. Using the Network Enforcement Act in Germany as an example, platforms are obligated under the law to enforce rules that reduce disinformation. At the same time, platforms are tasked with protecting user speech in both substantive and procedural dimensions. As meta-regulation is marked by the level of discretion it affords, the "trap" of over-regulating the platforms at the expense of reducing efficiencies would be avoided. Yang's piece thus challenges us to situate fundamental rights within its commercial realities, and to adopt regulatory innovation (which some might say is the province of lawyers).

10 The language of rights resurfaces again, this time in the context of data protection law (without which the special issue would be incomplete). Professor Michelle Miao in "Debating the Right to Explanation: An Autonomy-Based Analytical Framework" examines a specific and emerging right, the right to explanation ("RTE") that is believed to derive from the EU's General Data Protection Regulation ("GDPR"). As she argues and explains, this right is important in view of the shifts in power to tech companies and public institutions, and the risks and harms of today's algorithmic society: "There are few more robust and more straightforward power equalisers than knowledge and transparency."[4] Thus, the RTE is of interest not just because of how influential the GDPR is worldwide but also because the subject dovetails more broadly with debates on transparency and explainable AI.

11 Professor Miao sets about her task to resolve the controversies in construing the right[5] by exploring its potentials and limitations, and advancing an autonomy-based theory to conceptualise the right. Questions explored include: What does the right *not to be* subjected to automatic decision-making entail? Which algorithmically-made decisions fall under the provision? What is the quality of explanation

4 Professor Miao also points out that the RTE is often a gateway right to other transparency-related rights such as contest, correction and erasure, and hence is also "a precondition for data controllers to fulfil their legal and ethical accountability".

5 Five issues were discussed: (a) the legislative source of the right; (b) nature of the right (proscription *versus* entitlement); (c) context in which it applies (degree of automation required); (d) legal significance; and (e) quality of explanation required.

required under law (meaningfulness test)? Singapore lawyers would also appreciate that in Prof Miao's exploration of when humans are "in the loop" within the uncertain boundaries of human-machine collaboration, she referred to a Singapore case on algorithmic trading of cryptocurrency.[6] She also proposes a novel autonomy-based test to determine which modes of human–machine collaboration would be captured by the GDPR. According to Prof Miao, achieving the status of autonomy involves a two-pronged criterion: (a) the data subject having obtained awareness (of logics, mechanisms and consequences of automated decisions); and (b) possessing the capacity to make rational decisions. Examples, such as credit scoring, were given to illustrate how the approach would work.

12 Overall, understanding data control as "an extension of the autonomy of data subjects" is a convincing conceptualisation, and the theory resonates more broadly with debates on digital self-determination.[7] As jurisprudence has yet to emerge in one coherent voice, academic debates over the theoretical foundations of data governance and the explorations of new legal tools such as the RTE will be crucial.

13 Finally, Prof Gary Chan Kok Yew from the Centre for AI and Data Governance ("CAIDG") contributes a piece titled, "Mind the Gaps: Assessing and Enhancing the Trustworthiness of Mental Health Apps". Professor Chan uses a specific AI application, *ie*, mental health apps, to expose the regulatory risks, gaps and challenges in governing AI. This is a pertinent example because safety, efficacy and privacy concerns are all intensified in a mental health app. For example, if not designed with adequate safety measures, including suicide prevention strategies, the use of such apps can have dire consequences on one's well-being and life. The app's users, especially those with pre-existing mental health conditions, are particularly vulnerable.

14 Using mental health apps as the point of analysis also raises interesting observations. While emotional AI was earlier raised in Dr Pietropaoli's piece as an intrusive and contentious use of AI (*eg*, by social media platforms), some mental health apps similarly track users' symptoms and moods as part of their function. The use of AI in this healthcare setting reveals that technology should not be viewed as the enemy but should also be acknowledged for its potential to facilitate human flourishing. For instance, the use of mental health apps can protect its users from social stigma (associated with mental illness) while increasing accessibility to healthcare or information. On the human–

6 *Quoine Pte Ltd v B2C2 Ltd* [2020] 2 SLR 20.

7 "Digital Self-Determination" *Centre for AI and Data Governance* <https://caidg.smu.edu.sg/digital-self-determination> (accessed 21 September 2022).

computer interaction front, psychotherapy apps can produce more positive health outcomes as patients tend to be more honest and open in their disclosure to chatbots. However, Prof Chan also notes that privacy infringements can exacerbate the problem of stigma and mental harm associated with individuals with mental health conditions. Worryingly, Prof Chan reports instances of data being transmitted for advertising purposes without the users' knowledge.[8]

15 Thus, this all boils down to the prevailing research theme in the governance of emerging technologies: trust. Can we trust mental health apps? Examining this at the level of the AI application showcases the wider *ecosystem*: users (which can include patients and healthcare professionals), developers, regulators and other stakeholders. To enhance trust in mental health apps, Prof Chan suggests assessing their trustworthiness and acceptability by reference to regulatory, ethical and technological benchmarks. However, as the web of relevant local law and regulations (including data protection, advertising, negligence and possibly consumer protection) would be confusing for the average consumer, app developer and user, he calls for government, policymakers and different sectors to collectively develop an overarching regulatory framework for health apps. Further recommendations are given to promote transparency and to address key aspects of safety, efficacy and privacy. Finally, he recommends that the views of patients should be incorporated into the design of the app, and that clinicians need to be more involved at the app development stage to enhance the trustworthiness of the app.

16 This comprehensive examination of AI deployment in the healthcare sector is a very fitting end to this issue. From here, we would like to comment on common themes emerging from this special issue.

II. Thematic analysis

17 The first theme that emerges strongly is power. An illustrious example is social media platforms. Further, the pervasiveness of algorithms across all aspects of our lives, such as healthcare and credit loans, demonstrate our dependence on AI-assisted technology in this "algorithmic society". The authors have referred to both the growth in "technopower" and the shifts in power from individuals to tech companies and public authorities. There are areas of law that seek to

8 Regarding the business model of apps, Prof Chan also points out that "[i]n reality, the level of enforcement of apps store rules are also tied to financial incentives to accept and monetise the apps through targeted advertising".

address power asymmetries: competition law aims to balance market power (Dr Lestari calls for network effects and access barriers to big data to be considered), data protection law (such as the emerging right to explanation and transparency principles) can be seen as empowering data subjects, and constitutional and administrative law emphasises the non-interference of fundamental freedoms. However, as these authors have explained, existing legal frameworks are insufficient. Further, the cross-border nature of the digital age produces an additional layer of complexity, suggesting that some level of universality or harmonisation of laws will be important, even though enforcement will be carried out in the individual jurisdiction.[9] This provided the impetus for the CAIDG's research on the rule of law and COVID-19 control technologies (such as contact tracing apps), in search of an "ethics-plus" universal framework that could constrain arbitrary power while providing remedies to users.[10]

18 The flip side of power is of course disempowerment. As has been illustrated, the harms of AI-assisted technology tend disproportionately to afflict marginalised groups,[11] therefore, implementing algorithmic fairness in tandem with anti-discrimination laws is an urgent task. Considering legal and regulatory design from the lens of the vulnerable might also reveal to policymakers the gap between remedies and practice. For example, as Prof Miao astutely points out, seeking empowerment can be burdensome, particularly on individuals whose interests are adversely impacted. By requiring, under law, for individuals to have a level of awareness and capacity in order to trigger a remedy, when in practice they have none, could mean that the law inadvertently becomes a cover for entrenching inequalities and disempowerment.[12] Similarly, a singular focus on inequalities within national jurisdictions could obscure global

9 For instance, Dr Pietropaoli in her piece referred to a competition law class action suit in the UK involving 44 million Facebook users that claimed that their data had been exploited.

10 Jane Loo & Mark Findlay, "Rule of Law, Legitimacy, and Effective COVID-19 Control Technologies: Arbitrary Powers and Their Influence on Citizens' Compliance" *SMU Centre for AI & Data Governance Research Paper 03/2022*. See also the white paper produced in collaboration with the British Institute of International and Comparative Law and the Technical University of Munich: Julinda Beqiraj *et al*, *White Paper: Rule of Law, Legitimacy and Effective COVID-19 Control Technologies* (Technical University of Munich, July 2022). More information on this research collaboration project can be found at "Rule of Law, Legitimacy and Effective COVID-19 Control Technologies" *Bingham Centre for the Rule of Law* <https://binghamcentre.biicl.org/projects/rule-of-law-legitimacy-and-effective-covid-19-control-technologies> (accessed 21 September 2022).

11 See also Mark Findlay *et al*, "The Vulnerability Project: The Impact of COVID-19 on Vulnerable Groups" *SMU Centre for AI and Data Governance Research Paper 09/2021*.

12 This is a theme addressed in Mark Findlay, *Globalisation, Populism, Pandemics and the Law: The Anarchy and the Ecstasy* (Edward Elgar, 2021).

inequalities facilitated by AI. This is why the sustainable development agenda should be a focus of responsible AI initiatives.[13]

19 The second theme that emerges is the question of how power should be dispersed or governed. In this issue we have the following proposals: improving accountability through business and human rights, meta-regulation, and enhancing knowledge and transparency (whether at the point of downloading an app or exercising the right to an explanation). The theoretical foundations (rooted in human autonomy) of controlling and accessing one's data have also been covered.[14] In considering regulatory design, perhaps we should consider what we are governing. Is it power itself, in that no entity can be trusted to wield too much power? Is it an issue of addressing and correcting commercial incentives (*per* Yang) or is it about ensuring safeguards and accountability (*per* Dr Pietropaoli)? As data protection and self-determination can conflict at the boundaries (*per* Prof Miao), how do we resolve these tensions? Looking at it from another way, what responsibilities and duties do we owe each other in a digital space?[15]

20 This brings us to a third and final theme: trust. Black letter lawyers might find comfort in solely reading and interpreting law, but ignoring the socio-legal angle in the context of emerging technologies is ill-advised. Law and other regulatory instruments including ethics have a normative function, shaping what is acceptable and legitimate to users. Conversely, how can these instruments help to create safe digital spaces and as such facilitate trust from users?[16] Trustworthiness is the

---

13 Li Min Ong & Mark Findlay, "A Realist's Account of AI for SDGs: Power, Inequality and AI in Community" in *The Ethics of Artificial Intelligence for the Sustainable Development Goals* (Springer Nature, forthcoming). The CAIDG is also currently editing a handbook that promotes voices in the "Global South" on AI regulation and governance: *Handbook on Regulating AI and Big Data in Emergent Economies* (Edward Elgar, forthcoming).

14 On a related note, the theoretical foundations of digital self-determination have been explored in Nydia Remolina & Mark Findlay, "The Paths to Digital Self-Determination – A Foundational Theoretical Framework" *SMU Centre for AI and Data Governance Research Paper 03/2021*.

15 The question of what we owe each other is explored in the CAIDG's digital self-determination project under the wider "AI in Community" initiative that promotes a communitarian approach to data governance: "SMU's Centre for AI and Data Governance Launches New Research, Policy and Community Outreach Initiative to Improve Human-AI Exchanges" *SMU Newsroom* (17 June 2021) <https://news.smu.edu.sg/news/2021/06/17/smus-centre-ai-and-data-governance-launches-new-research-policy-and-community> (accessed 22 September 2022).

16 Laws and regulatory instruments can help to protect the safety of digital spaces and accommodate duties for respectful engagement for digital self-determination: Mark Findlay, *12 FAQs on Digital Self-Determination* (Centre for AI and Data Governance, 25 February 2022) <https://caidg.smu.edu.sg/sites/caidg.smu.edu.

(cont'd on the next page)

discourse that dominates the tech field, as companies are recognising that the buy-in of users is needed in order for them to adopt AI-tech. AI ethics is intertwined with this discourse. To facilitate trust, ethics including variables like algorithmic fairness need to be translated across the whole AI ecosystem of stakeholders[17] and needs to be contextualised to the community of users.[18] Trust also needs to be examined beyond the passive frame of a technology's "trustworthiness" to encompass the dynamics of users' trust.[19] As such, users' and stakeholders' trust can be seen as a regulatory frame, helping to bridge the gap raised by Dr Pietropaoli between ethics and practice. Contemporary discourse on participation in tech design by users, as raised by Prof Chan, is hence promising because co-design may not only help drive tech innovation but also enhance stakeholders' trust.

21 We are grateful to our authors, who are based in Singapore, Hong Kong, Taiwan, Indonesia and the UK; their contributions illustrate that the issues are cross-cutting and international. We are enriched by their perspectives and without their contributions, this issue would be lacking in coverage and the picture painted would not have been nearly as nuanced. We hope you enjoy this issue.

---

sg/files/12%20FAQs%20on%20Digital%20Self-Determination.pdf> (accessed 21 September 2022).

17 "AI Ethics Hub 4 Asia" *Centre for AI and Data Governance* <https://caidg.smu.edu.sg/thehub> (accessed 21 September 2022).

18 Mark Findlay & Willow Wong, "Kampong Ethics" in *Reframing AI Governance: Perspectives from Asia* (Digital Futures Lab & Konrad-Adenauer-Stiftung, 2022).

19 The CAIDG has advanced a "decision-to-trust" model that looks at trust as an active process: Wenxi Zhang, Willow Wong & Mark Findlay, "Trust in Robotics: A Multi-Staged Decision-Making Approach to Robots in Community" *SMU Centre for AI and Data Governance Research Paper 01/2022*.