KHAZANAH
RESEARCH
INSTITUTE

VIEWS 5/23 | 6 MARCH 2023

Addressing Data-centred Rights: Protecting Our Digital Doubles

Jun-E Tan

The rapid advancement of digital technologies presents a multitude of novel and complex challenges to the protection of human rights, especially violations that cut across the digital and physical. In this article, I offer a conceptual framework for digital rights in general and from there, zoom into data-centred rights, one of the less-discussed aspects of digital rights, which deserves more attention for the societal implications for years to come.

Conceptual framework for digital rights

One of the problems of advocating for digital rights is a lack of consensus of what the concept means. In 2019, I conducted a study interviewing 24 digital rights advocates and activists from Malaysia, the Philippines and Thailand, and built a

Views are short opinion pieces by the author(s) to encourage the exchange of ideas on current issues. They may not necessarily represent the official views of KRI. All errors remain the authors' own.

This view was prepared by Dr Jun-E Tan, a researcher from the Khazanah Research Institute (KRI). The author is grateful for the valuable comments from Dr Rachel Gong.

Author's email address:
june.tan@krinstitute.org

An earlier version of this article was published in ISIS Focus 12/2022 No. 17, titled "Data-centred rights to the forefront".

Information on Khazanah Research Institute publications and digital products can be found at www.KRInstitute.org.

Cover photo by Andy Kelly on Unsplash.

conceptual framework to encapsulate four main spheres of digital rights.[1]

The four spheres of digital rights are as follows: 1) conventional human rights[2] translated to digital spaces, 2) data-centred rights, 3) rights to access digital spaces and services, and 4) rights to participate digital governance.

The study found that within Southeast Asia, the digital rights movement focused mostly on the dimension of human rights translated to digital spaces, notably on issues such as freedom of expression and online gender-based violence. Access to the digital was not a key focus, possibly because governments in the region had prioritised digitalisation and connection. Participating in digital governance was mainly at national or subnational levels on influencing government policy on ICT, with forums for international standards setting mostly out of reach.

Data-centred Rights

Data-centred rights, also a peripheral issue at that point, was just starting to appear as part of the discourse, with few civil society organisations working on raising awareness about why data privacy and security was important. It is not an easy point to articulate, that a set of data points would constitute a "digital double" of oneself (or one's car, or one's city, etc), which could be used to make high level decisions that could act against or for the individual's rights or living conditions.

From one angle, with the relentless datafication of ourselves and our lives, such as online activity, biometric data of various parts of our bodies, our medical and financial data, and even how we move and breathe with the advent of the metaverse - our digital doubles have become more and more comprehensive representations of us. From another, data-driven artificial intelligence (AI) systems such as machine learning software are increasingly used to mine insights and automate decision-making in different fields.

As we stand in 2023, this area of digital rights is still quite underdeveloped in the region, even when risks and harms rise in importance as AI technologies permeate our everyday life. Our online interactions are mediated by recommendation systems offering personalised content (such as social media feeds and online shopping); and offline, our movements are increasingly digitised and tracked and monitored by corporations and government bodies.

For instance, in Malaysia, we already see some of these technologies in use to provide public services, such as the Penang state government using facial recognition technology for CCTV surveillance to combat crimes[3], or the court systems in Sabah and Sarawak piloting predictive

[1] Tan (2019)
[2] As outlined by the Universal Declaration of Human Rights
[3] Mok (2019)

statistical analysis, with the intention to move towards machine learning, to assist in decisions on sentencing for drug and rape offences[4].

While there has been little reporting on the efficacy and safety of these systems in the Malaysian context, similar implementations elsewhere have raised concerns, such as facial recognition systems[5] and risk recidivism software[6] in use in the US amplifying racial biases and marginalising the marginalised further. Another example of decision-making based on data and digital bodies that has an outsized impact on society is the social credit systems in China, which rate the behaviour of citizens, companies, and even government agencies, and offer rewards or punishments accordingly.[7]

Governance of Data and AI Applications

There are at least two ways to view this problem of protecting data-centred rights. The first is to protect the data itself, and this includes comprehensive policies and procedures of data governance to protect data privacy and security, typically managed at an organisational level. The scope of data covered should not be limited to personal data representing people, but also non-personal data and metadata from which inferences can be made.

The second is to govern the applications that make use of this data. In 2021, the European Union released a draft of its proposed Artificial Intelligence Act[8], which may set a worldwide standard for AI regulation (as did the General Data Protection Regulation, or GDPR, for data protection). Notably, the Act classifies and regulates applications by level of risk imposed on EU citizens by any AI application.

Applications that pose "unacceptable risk" such as subliminal manipulation and exploitation of vulnerable groups, or social credit scoring by public authorities, or real-time biometric identification systems in public spaces, are proposed to be prohibited outright. "High risk" applications (e.g. applications for recruitment, assessing consumer creditworthiness, safety-critical systems, etc.) will be subject to more regulatory oversight than "low or minimal risk" applications (e.g. AI chatbots, spam filters, and most other AI systems).

As with most initiatives like this, the devil is in the details, and many have offered in-depth analyses and critiques about what is proposed.[9] In general, it is a good move away from industry self-regulation, as well as narrowly defined[10] and poorly applied[11] AI ethics. Situating AI

[4] Khazanah Research Institute (2021)
[5] Najibi (2020)
[6] Larson et al. (2016)
[7] Lee (2020)
[8] European Commission (2021)
[9] Future of Life Institute (n.d.)
[10] Tan (2020a)
[11] Tan (2020b)

technologies in their application and societal contexts, with a risk-based approach, is an important step to add another layer of protection to data-centred rights.

Conclusion

A conceptual breakdown of digital rights offers us a clearer clarity of the problem areas, and we see that each sphere of digital rights comes with its historical context and stakeholders, as well as existing research and advocacy issues. The breadth of what is covered can then be mapped out, to address gaps and form bridges among state and non-state actors.

While all spheres of digital rights are important and have real life implications, the area of data-centred rights is the least-understood and the fastest growing. In keeping with the global AI regulatory landscape, as Malaysia moves ahead with its National AI Roadmap, Digital Economy Blueprint, and National Fourth Industrial Revolution (4IR) Policy, it will also have to ensure that data and AI regulatory structures are in place to protect its citizens, so that risks of the technologies do not outweigh their benefits.

References

European Commission. 2021. "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts." April 21, 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

Future of Life Institute. n.d. "Analyses." The Artificial Intelligence Act. Accessed February 15, 2023. https://artificialintelligenceact.eu/analyses/.

Khazanah Research Institute. 2021. "#NetworkedNation: Navigating Challenges, Realising Opportunities of Digital Transformation." Kuala Lumpur: Khazanah Research Institute.

Larson, Jeff, Surya Mattu, Lauren Kirchner, and Julia Angwin. 2016. "How We Analyzed the COMPAS Recidivism Algorithm." ProPublica. May 23, 2016. https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

Lee, Amanda. 2020. "What Is China's Social Credit System and Why Is It Controversial?" South China Morning Post. August 9, 2020. https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial.

Mok, Opalyn. 2019. "Penang Launches Country's First Facial Recognition CCTV Surveillance." *Malay Mail*, January 2, 2019, sec. Malaysia. https://www.malaymail.com/news/malaysia/2019/01/02/penang-launches-countrys-first-facial-recognition-cctv-surveillance/1708422.

Najibi, Alex. 2020. "Racial Discrimination in Face Recognition Technology." Science in the News, Harvard University Graduate School of Arts and Sciences. *Racial Discrimination in Face Recognition Technology* (blog). October 24, 2020.

https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

Tan, Jun-E. 2019. "Digital Rights in Southeast Asia: Conceptual Framework and Movement Building." In *Exploring the Nexus between Technologies and Human Rights: Opportunities and Challenges for Southeast Asia*, edited by Ying Hooi Khoo and Deasy Simanjundtak. Bangkok: SHAPE-SEA.

———. 2020a. "A Critical View of AI Ethics: Looking at the Substance of Ethical Guidelines." *EngageMedia* (blog). August 10, 2020. https://engagemedia.org/2020/artificial-intelligence-ethical-guidelines/.

Tan, Jun-E. 2020b. "Problems in Putting Principles into Practice: A Critical View of AI Ethics." *EngageMedia* (blog). August 17, 2020. https://engagemedia.org/2020/artificial-intelligence-ethics-in-practice/.