AI, Data and Private Law – Translating Theory into Practice

Duarte Nicolau, Tatiana

Published in:
European Data Protection Law Review

Publication date:
2022

Book Review

The Book Reviews section will introduce you to the latest and most interesting books on a wide range of topics pertaining to the law and policy of data protection. For further information on the submission of reviews please contact the Book Reviews Editor Gloria González Fuster at Gloria.Gonzalez.Fuster@vub.be.

AI, Data and Private Law – Translating Theory into Practice

By Gary Chan Kok Yew and Man Yip (eds)
Hart Publishing 2021 (286 pp.)
£90.00

*Tatiana Duarte**

AI, Data and Private Law – Translating Theory into Practice is a collection of articles resulting from the Conference 'AI and Commercial Law: Reimagining Trust, Governance, and Private Law Rules', held at the School of Law of Singapore Management University on 5-6 December 2019.

The work is structured in two Parts, the content of which is thoroughly introduced to the reader by the editors, Gary Chan Kok Yew and Man Yip, both Professors of Law with a keen interest and experience in the domain of private law. While Part one comprises a critical appraisal of South Korea, Singapore and Malaysia legal regimes and governance solutions for the protection of personal information, Part two focuses on specific technologies and corresponding regulatory models in a batch of jurisdictions.

The editors state that the work has two aims: first, to demonstrate that private law concepts and doctrines afford interpretative tools to think and regulate new technologies; second, to follow a theoretical approach that addresses practice, focusing on (without being restricted to) Asia-Pacific jurisdictions.

Although not all articles centre strictly on private law, it shows that private law is a resourceful basis to interpret and regulate innovation, both by exploring existing concepts and institutions – such as tort law, contract law, fiduciary law, liability, property, negligence – and by proposing new ones, such as *data trusts* and *information fiduciary*.

Beyond (and within) strict private law domain, the book proposes data governance instruments and illuminates relevant practical questions concerning the regulation and implementation of technology. Such questions involve the extent to which technological affordances constrain and challenge law, and the interpretative difficulties that stem from the fluidity of legal concepts.

The book succeeds in accomplishing its aims, while providing a sample of the academic and regulatory landscape within the targeted jurisdictions, with an observable prominence of Singapore.

The first chapter of Part one is entitled "How to De-identify Personal Data in South Korea – An Evolutionary Tale". Ko and Park report on the South Korean legal approach to the protection of personal information through the lenses of the concepts of *de-identification* and *pseudonymisation*. The latter concept was introduced by what the authors dub "the 2020 Amendments",[1] as an alternative to the prior controversial scheme of de-identification, which was a condition to engage certain kinds of processing activities.

Although the GDPR influence on the South Korean construction of pseudonymisation is tangible, the current regime has idiosyncrasies that make it a different *animal* from the one emerging from the GDPR. While in the GDPR pseudonymisation is essentially a safeguard, in the South Korean legal regime pseudonymisation is one of the requirements to engage in certain processing activities (in line with the former de-identification).[2] This chapter traces the conceptual development from de-identification to pseu-

DOI: 10.21552/edpl/2022/1/23

* Tatiana Duarte, Doctoral researcher at Law Science and Technology and Society Studies (LSTS), Vrije Universiteit Brussel (VUB), Belgium. For correspondence: <tatiana.duarte.nicolau@vub.be>

1 Referring to the amendments to the following acts, approved in (and in force since) 2020: (i) Personal Information Protection Act (PIPA), (ii) Act on the Protection and Utilization of Credit Information and (iii) Act on the Promotion of Information and Communications Network Utilisation and Information Protection. Haksoo Ko; Sangchul Park, 'How to de-identify personal data in South Korea – An evolutionary tale' in Gary Chan Kok Yew and Man Yip (eds.) *AI, Data and Private Law – Translating Theory into Practice*, Hart Publishing 2021, 34.

2 Ibid 44.

donymisation, identifying interpretative uncertainties in their practical application.

In "Data Trusts for Lawful AI Data Sharing", Reed proposes data trusts as a governance scheme, with the competence to issue binding rules for the regulation of each singular instance of data sharing.[3] In such regime, data can only be shared for a specific and specified purpose that limits what the recipient can do with the data, regardless of whether (non-)personal data is involved.[4]

As proposed, data trusts are a tailor-made, rule-based structure for each data sharing occurrence, legally separate from those who share data among themselves – not so much in the private law sense of *legal trusts*, but rather as a *trustful* (and hopefully *trusted*) mechanism to promote data sharing.[5]

"The Future of Personal Data Protection Law in Singapore: A Role for the Use of Al and the Propertisation of Personal Data", by Warren Chick, and "Personal Data as a Proprietary Resource", by Pey Woan Lee, present a similar reasoning about the qualification of personal data as property under the Singaporean Personal Data Protection Act (PDPA) – albeit acknowledging that such proposal is not provided for by the legislature nor supported by nationally recognized interpretative bodies.[6]

Chick suggests that the canonical proprietary rights *to exclude* and *to control* have equivalents in the GDPR, the former materialized on consent and on the right of erasure – which allow the exclusion of others from processing – and the latter on the right of portability – which allows data subjects to choose whom they want to process their data.[7] The chapter argues that, by reinforcing data subject's control over their personal information, EU law has embraced a more proprietary perspective concerning personal data.[8]

The dogmatic ground of Chick's thesis resides on the *erga omnes* efficacy of property rights, which, it is argued, if extended to personal data, would enhance legal protection.[9] Lee states that the legal institution of property enhances data subjects' control over their personal information.[10] Such form of property would be *sui generis*, as it could only be partially alienable.[11]

For the European reader, *control over personal information* does not necessarily (indeed, does not) imply an incident of ownership of property, but rather a fundamental right of making decisions about external (non-domestic) acts of personal information processing. As the chapters do not consider the European Union law conceptualization – where all property is (also) about control, but not all control is about property –, they suggest that only through *property* can individuals expect *control*.

"Transplanting the Concept of Digital Information Fiduciary?" proposes that the concept of information fiduciary might usefully be adopted in Singaporean and Malaysian jurisdictions. Yip grounds this proposal both on a general understanding of fiduciary law and on a paradigmatic and contextual dimension of the fiduciary relation (i.e., doctors).[12] The *information fiduciary* is both a creative development of the concept of *fiduciary* and a practical mechanism intended to bring over flexibility and enhance legal protection – both by filling in the gaps of the law and by

3 Chris Reed, 'Data Trusts for Lawful Data Sharing' in *AI, Data and Private Law* 56-57.

4 Ibid 52.

5 Ibid 68.

6 Warren Chick, 'The Future of Personal Data Protection law in Singapore - A Role for the use of Al and the Propertisation of Personal Data' 70. Pey Lee, 'Personal Data as a Proprietary Resource' 109 in *AI, Data and Private Law*, 107.

7 Warren Chick, ibid 85-86.

8 Ibid 81.

9 Ibid 83-84. It could, however, be said that the *erga omnes* efficacy is not a decisive argument in favour of propertisation, especially for those who consider the protection of personal data protection as a fundamental right. However, that is not necessarily the case for Singaporean PDPA, which is crucial for understanding the reification of personal data as proposed by the authors. Nonetheless, out of the EU law framework, fundamental rights have already been qualified as *erga omnes*. In the context of International Law, human rights (what the International Court of Justice considered to be basic rights of the human person) were qualified as obligations of a State towards the international community as a whole, i.e., *erga omnes*. *Barcelona Traction, Light and Power Company* (*Belgium v. Spain*) (Judgment) [1970], I.C.J. Rep. 3, para. 33-34. To be sure, this does not mean that the International Court of Justice was referring to privacy or data protection. The point is that the *erga omnes* efficacy has already been attributed outside of property rights. Also, Yoram Dinstein, 'The Erga Omnes Applicability of Human Rights' in Archiv des Völkerrechts 30. Bd., No. 1, Drittstaaten und Sanktionen im Völkerrecht / Third States and Sanctions in Public International Law (1992) 16.

10 A similar argument seems to have been made by Lawrence Lessig, 'Privacy as Property', in Social Research, Vol. 69, No. 1, Privacy in Post-Communist Europe (2002) 247, 260, 265.

11 Pey Lee, 'Personal Data as a Proprietary Resource' in *AI, Data and Private Law*, 113.

12 The context-based approach to fiduciary relation is inspired on the work of Jack Balkin, proposed at 'Information Fiduciaries and the First Amendment' in UC Davis Law Review Vol. 49 No. 4 (2016) 1183.

supporting better regulatory standards and commercial practices.[13] The theoretical attribution of fiduciary duties to the *information fiduciary* comes from a refutation of information as property,[14] which seems to counter the accounts stated on Chick and Lee's articles. If so, that only means that the book is enriched by diverse theoretical underpinnings, reflecting the permanent debate inherent to law.

"Regulating Autonomous Vehicles: Liability Paradigms and Value Choices" presents an overview of the liability paradigms for regulating autonomous vehicles in four Asia-Pacific jurisdictions (Singapore, Australia, New Zealand and Japan) and compares them with the regulatory approaches in the United Kingdom and the European Union. The research question that informs the article is the extent to which current laws and liability paradigms need to change to cater for autonomous vehicles. Siyuan dedicates particular attention to Singaporean legislative approach to autonomous vehicles, noting that, although it is still rather limited, it cautiously prioritizes safety and accountability.[15] The article suggests that the adoption of strict liability systems may be justified in cases where it is extremely onerous for regulators to verify autonomous vehicles' software.[16]

In "Medical Al, Standard of Care in Negligence and Tort Law", Yew invites the reader to join an investigative journey that includes an inquiry into the content of the standard of care and policy considerations on doctor's and hospital's liability in Singapore and Malaysia.

The author argues that negligence is a potential standard for balancing risks and benefits, claiming that its adaptiveness fits the regulatory needs concerning the use of AI for medical diagnosis and treatment.[17]

"Contractual Consent in the Age of Machine Learning", by Goh Yihan, explores the nature, the value and the regime of the expression of contractual will in the context of algorithmic contracts.[18] The articles assesses such contracts against two legal paradigms, namely the law of formation and the law of mistake. It concludes that the adaptation of current legal mechanisms can offer satisfactory regulation for algorithmic contracts.[19]

In "Digital Assets: Balancing Liquidity with Other Considerations", Acrich, Litvak, Dvori, Samuelov and Greenbaum discuss the key features of a typology of digital assets under US law, highlighting issues related to ownership, inheritance and privacy. The authors focus on the tokens that run on top of the Ethereum protocol. They argue that Initial Coin Offerings (ICO) tokens should be considered a unique kind of asset, the taxation of which heavily depends on tax classification.[20] The chapter proposes a mixed regulatory solution for tokens, involving an international treaty, mechanisms of self-regulation and market forces.[21]

"Blockchain in Land Administration? Overlooked Details in Translating Theory into Practice" challenges the reader to reflect on the congruence of blockchain affordances with legal norms on land administration. The author argues that the characteristics of public blockchains are not adaptive to the theoretical and practical needs of land administration, as no property system subscribes to absolute immutability.[22]

Conversely, private blockchains may be configured to allow the alteration of information, thereby trading immutability for control. Such flexibility allows the current trade-offs between rigour, transparency and defeasibility to be represented on the blockchain.[23]

Overall, the book opens the reader's horizons,[24] regardless of their (non-)expertise on the covered legal systems, or on the technologies addressed. The plasticity of law is revealed throughout the book, whether through interpretation of existing legal solutions or through inventive constructions, making of it an inspiring expression of human creativity.

---

13 Man Yip, 'Transplanting the concept of Digital Information Fiduciary?' in *AI, Data and Private Law*, 143.

14 Ibid., 126, 141.

15 Chen Siyuan, 'Regulating Autonomous Vehicles: Liability Paradigms and Value Choices' in *AI, Data and Private Law*, 151.

16 Ibid 171-172.

17 Gary Yew, 'Medical Al, Standard of care in Negligence and Tort law' in *AI, Data and Private Law*, 182, 193, 198.

18 The chapter uses the umbrella term 'algorithmic contracts', comprising smart contracts, but also those that use algorithms to conclude their terms without executing them.

19 Goh Yihan, 'Contractual consent in the Age of Machine learning' in *AI, Data and Private Law*, 223.

20 Gal Acrich et al., 'Digital Assets – Balancing liquidity with other considerations' in *AI, Data and Private Law*, 248.

21 Ibid 249-251.

22 Alvin W-L See, 'Blockchain in Land Administration? Overlooked Details in Translating Theory into Practice' in *AI, Data and Private Law*, 255-259, 272.

23 Ibid 258, 272.

24 In the sense patented in Georg Gadamer, *Truth-and-Method*, Second, Revised Edition Translation revised by Joel Weinsheimer and Donald G. Mars, Continuum (2004) 313-318.