Book Reviews

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.

Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way
by Virginia Dignum
Springer 2019, pp. 127.
€ 42.79; Hardcover / € 32.09; eBook

*Andreas Ebert**

Artificial Intelligence (AI) has been one of the hottest topics in and outside of the global scientific community in the last few years. Not a single day goes by without a new word on how AI is changing our lives. AI, however, is not always AI – or at least not what many people believe it is. In her new book *Responsible Artificial Intelligence*, Virginia Dignum strives out to analyse what responsibility means in the context of AI, and provides essential guidance on how to design and develop AI in a responsible way. Despite the technical background of the author,[1] the book is written from an interdisciplinary perspective. Beyond being able to understand some smaller bits such as the description of an algorithm in pseudocode,[2] it is not necessary to have any deeper technical knowledge on the subject to read the book. On the contrary, the volume illustrates comprehensibly what AI actually is, as well as what it is capable of, and provides the theoretical foundations for further reasoning.

Describing what AI is can be difficult and overwhelming. It comes as no surprise, thus, that the author dedicates an entire chapter (2) to the concept of AI as a means and as a discipline. She demonstrates the various streams within AI research, and illustrates how different disciplines such as computer science, philosophy and psychology, among others, approach AI systems. The book lastly defines intelligence as 'the ability to *do* the right thing at the right moment', whereas AI is considered the discipline that 'studies and develops computational artefacts that exhibit some facet(s) of intelligent behaviour'.[3] These artefacts are also referred to as *(artificial) agents*.[4] In this context, a particular emphasis is laid on the description of *AI agency* as proposed by Luciano Floridi,[5] a concept which will accompany the reader throughout the book. From this viewpoint, agency consists of three principal characteristics: *autonomy*, or the ability of agents to decide how they act; *adaptability*, which describes the process of learning from changes effected in the environment, and *Interactivity*, or the capacity of interacting with other agents to coordinate activities in that environment.[6]

Following such presentation, the author delves into the basics of ethical decision-making (chapter 3). Whether a certain decision may be deemed 'ethical' or not depends on the underlying values, which in turn depend on diverse factors, such as the socio-cultural background of a person.[7] The author names three main theories for (normative) ethical reasoning: *consequentialism*, *deontology* and *virtue ethics*.[8] She then illustrates their differences in outcomes through the means of the classic moral dilemma in which an autonomous vehicle must decide between two actions which are both harmful for different

DOI: 10.21552/edpl/2020/4/22

* Andreas Ebert is a Doctoral Researcher at Goethe University Frankfurt within the project 'RoboTrust', which is funded by the Hessian Center for Responsible Digitalisation, as well as at Karlsruhe Institute of Technology in the IT-security project 'KASTEL', funded by the German Federal Ministry of Education and Research. For correspondence: <ebert@jur.uni-frankfurt.de>.

1 Virginia Dignum is a Professor at the Department of Computer Science at Umeå University.

2 Virginia Dignum, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way* (Springer 2019) 73.

3 ibid 17.

4 ibid.

5 Luciano Floridi, *The ethics of information* (Oxford University Press 2013), as quoted in Virginia Dignum (n 2) 17.

6 Virginia Dignum (n 2) 52.

7 ibid 35.

8 ibid 37-39.

groups of people. In a further step, the book proposes a pathway for implementing ethical reasoning in AI systems: after recognizing an event which requires action and acknowledging its ethical dimension, an agent must not only actively take ethical responsibility, but also identify and apply abstract ethical rules, and come to a solution before it finally acts.[9]

Having presented these basics, the author divides the subsequent chapters into three different applicational areas for ethics which are relevant during and after the conceptualization of AI systems: ethics *in* design, ethics *by* design, and ethics *for* design(ers).[10]

Ethics *in* design (chapter 4) mainly comprise the process of designing AI systems. In this regard, the book proposes the so-called ART principles for Responsible AI, an acronym which refers to Accountability, Responsibility (here in a narrower sense, referring to the role of people when developing or using an AI system) and Transparency.[11] The volume goes into detail on how these principles may be executed, and presents a value-driven approach to design which could be particularly helpful to achieve 'ARTful' AI.

Ethics *by* design (chapter 5) focus on the behaviour of AI systems and whether machines are actually capable of taking ethical decisions. Ethical reasoning may be developed in a computational infrastructure by using a variety of approaches. The book discusses three of them, and assesses their practicability, in particular taking into account the aforementioned ethical theories. Based on this analysis, it presents ways to implement ethical deliberation which range from strict algorithmic decision-making to randomness, and discusses how different levels of ethical behaviour are to be expected from different systems, such as a search engine or a personal assistant. Simultaneously, the author discusses whether such systems should be developed at all, and how the ethical status of an AI system itself can be determined. The author criticizes the fact that current discussions focus themselves too much on viewing AI as a separate entity, rather than considering it as a bigger field, which disregards the 'increasingly distributed and networked nature of AI'.[12] Finally, she deems the original question of whether AI systems can be ethical to be 'elusive', and calls for a formalization of the concept of responsibility.[13]

Ethics *for* design(ers) (chapter 6) try to make sure that all stakeholders involved in the process of conceptualization and in the use of AI themselves act in a responsible way. To this end, governance mechanisms can be deployed by national authorities, international bodies or private initiatives. The main instruments for ensuring governance are the regulation of AI development and use, but also certification. Codes of conduct could be used as a method of self-regulation by professional societies or enterprises themselves, she notes. Ultimately, she puts forward that AI development must surpass societal borders. On the one hand, this means that diversity and inclusion in all their facets should be taken into account during the conceptualization of AI.[14] On the other hand, in order for society to participate in the development process, it must be commonly understood what AI is, and how it works.[15] For this to happen, education and transparency play a vital role.

In the last chapter (7), the author analyses how AI could impact societies in different fields such as the labour market and education, before concluding with a comment on *superintelligence*, in which she scrutinizes the plausibility of the concept.

As a whole, the book serves as an excellent resource to grasp the impact and risks of AI development and use. Despite its apparent brevity, the book manages to give the reader a broad overview over the most relevant aspects of responsible AI in a clear and concise manner, leaving them with a clear vision of why it is important that society as a whole decides on how AI is used for the common good. At the same time, the work conveys an understanding of the fundamentals necessary for own deliberation, and demystifies the sometimes maybe a little bit fear inducing concept of AI in a good way. Dignum accomplishes this independently of the reader's background, which is essential to the book's spirit: to impart the interdisciplinarity of the subject.

9 ibid 44, 45.
10 ibid 6, 7.
11 ibid 52-54.
12 ibid 91.
13 ibid 91, 92.
14 ibid 101.
15 ibid 104.

Of Privacy and Power: The Transatlantic Struggle over Freedom and Security
by Henry Farrell, and Abraham L. Newman
Princeton University Press 2019; 248 pp
£25.00 / $29.95; Hardback

*Maria Magierska**

The persistent clash between two data titans,[1] the European Union (EU) and the United States (US), has been analyzed so often in fixed dualistic terms that it seems almost impossible to think beyond them. We got used to comfortable sets of dichotomies explaining the recurring divide. It is always either the EU or the US: dignity or liberty,[2] privacy or security,[3] unification or fragmentation, regulation or deregulation. In *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security,* Henry Farrell and Abraham L. Newman put these simplifying views into question. Rather than looking at the US and the EU as monolithic antagonists, they investigate by what means different actors influence the track of negotiations. As the authors demonstrate, opposing views are present on both sides of the Atlantic. The final outcome of transatlantic developments is not only the result of talks between the European Commission and the American government but also of interdependences existing on many different levels: involving privacy activists, lobbyists, politicians and even contradictory interests of European Commission's Directorates-General. Each group has its own goals that very often go across the simple divide between a privacy-obsessed Europe and a security-oriented US.

The book is divided into five parts. In the first chapter, the authors explain the theoretical framework of their analysis. Subsequently, they summarize the history of the transatlantic dialogue and disagreement around data transfers throughout the years. Three chapters focus then on case studies: the debates around the Passenger Name Record (PNR) data, the negotiations of the EU-US SWIFT agreement, and the clashes after the invalidation of the Safe Harbour Privacy Principles by the EU Court of Justice in 2015. The authors conclude with remarks about the future of transatlantic relations.

To explain emerging multilateral, cross-national relations, Farrell and Newman develop a theoretical framework – the New Interdependence Approach (NIA).[4] Instead of considering transatlantic politics as 'a system clash', they propose focusing on 'intersocietal interactions, in which globalization creates opportunities for 'transnational actors' to shape international politics'[5]. Going beyond the state vs. state approach allows recognizing global and often opposing communities that use various strategies to achieve their goals, not only on domestic levels, but also on a worldwide scale. In the globalized world where the overlapping of multicentric legal orders becomes regular, non-state entities are also part of the debate, and these new dynamics open for innovative coalitions of different types of actors.

Especially noteworthy is how Farrell and Newman trace the use of networks by different groups in order to exercise power. They distinguish between *change actors,* that would like to revolutionize existing institutions, and *status quo actors,* that want to protect them.[6] Each group may have either low or high access to the transnational level, and, depending on this, they may exercise four different strategies: *defend and extend*, *cross-national layering*, *insulation* and *challenge.*[7] It may be questioned whether this classification is sufficient, and whether these tactics have only four different incarnations. In any case, according to the authors, frictions do not always lead to a fixed end with 'absolute winners and losers'. Instead, what is at stake is 'an ongoing process of contestation'[8]. The clear implication is that interdependence unceasingly enhances conflicts, but also creates opportunities.

Following the NIA, Farrell and Newman frame the clash between the US and the EU as a disagreement between 'privacy actors' and 'security actors'. In what

DOI: 10.21552/edpl/2020/4/22

* Maria Magierska is a Ph.D. researcher at the European University Institute in Florence, Department of Law. For correspondence: -lt--maria.magierska@eui.eu>.

1 A. Charlesworth, 'Clash of the Data Titans? US and EU Data Privacy Regulation', (2000), 6, European Public Law, Issue 2, pp. 253-274.

2 J.Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (Rochester, NY: Social Science Research Network, 5 December 2003).

3 R. A. Miller, *Privacy and Power a Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press 2017).

4 H. Farrell and A. Newman (2016) 'The new interdependence approach: theoretical development and empirical demonstration', Review of International Political Economy, 23:5, 713-736.

5 H. Farrell, and A. L. Newman*, Of Privacy and Power, The Transatlantic Struggle over Freedom and Security*, (Princeton University Press 2019) 26.

6 Ibid 28.

7 Ibid 30.

8 Ibid 37.

constitutes the most insightful part of their book, the authors demonstrate how the real divide is not between the US and EU, but between privacy- and security-oriented experts, politicians and activists on both sides. Instead of asking what was negotiated, they ask who the negotiators were. The answer is not that surprising: it was, originally, those who had been invited to the negotiations. For a long time, these were mostly members of the security community. In the most recent years, however, the privacy community developed new strategies that allowed it to become a part of the debate – even without an invitation. Farrell and Newman persuasively examine how this became possible.

As the book concentrates on the in-depth analysis of three mentioned case studies, the authors insightfully recapitulate what has already been broadly discussed in other works in the field: the evolution of data protection laws in Europe and the US from the 1980s until today, the impact of 11th September 2001 and of the 2013 Snowden's revelations, and, finally, the major incidents and documents of each case study. For someone who has already followed these debates, their summary may not reveal any new facts. What is original in this context, however, is the shift from the state-oriented approach towards the network perspective. Farrell and Newman focus on interchanging dynamics that drifted power from the proponents of security to the advocates of civil rights. Switching the attention to particular people behind the scenes complicates the picture, but also explains why the underlying problem has not yet been solved despite the attempts of so many.

The authors convincingly prove that a pro-surveillance stance usually associated with the US was also present in the agenda of the key EU's actors responsible for negotiations around PNR and SWIFT transfers. Dissatisfied with the EU stringent data protection laws, these actors used their exclusive access to cross-national negotiations in order to transform them. As Farrell and Newman demonstrate, EU and US security-oriented actors united and, as a result, achieved solutions satisfactory for the values of their community in the form of transatlantic agreements and changes to domestic laws, and this despite the strong opposition from privacy-oriented groups that, at that time, did not have sufficient access to the negotiations.

The power shift became possible only after Edward Snowden revealed how the US National Security Agency (NSA) had access to data of EU citizens that were using American digital services. The information published by the whistle-blower served a crucial evidence in the *Schrems* case that drastically transformed the landscape of transatlantic data transfers, and resulted in the EU Court of Justice's famous decision.[9] The authors meticulously examine debates around the proceedings, as well as the negotiations leading to the Privacy Shield, and the most distinct attitudes of the interested actors. They argue that privacy-oriented politicians and activists aimed to insulate the domestic level from external influence by using domestic political institutions.[10] The CJEU, by sharing almost completely the perspective of privacy activists, set a new direction. For the authors, the most important result of *Schrems* was that a previously neglected community gained visibility and audibility in the debate;[11] quoting one of the negotiators, 'there was much more solidarity and cohesion amongst the EU after the *Schrems* judgement'.[12] This immensely important observation tends to escape the attention of European scholars. The ruling had an unprecedented impact not only on the legal framework, but also on the unification of diverse viewpoints within the EU.

Reading this book barely a year after its publication, and yet already after a major thunderstorm of *Schrems II* decision,[13] it is hard not to agree with Newman and Farrell that the transatlantic debate is, indeed, an ongoing process of contestation. Although the CJEU unsurprisingly shared the perspective of privacy activists and continued the defined path, discussions have not been silenced. On the contrary, they erupted on a wider scale on both sides of the Atlantic. What is noticeable is that apart from the 'security community' and 'privacy community', another group has emerged – the one that puts commercial interests in the centre of its attention. Divergent opinions on how to tackle the problem appear even among the EU data protection authorities. The lack of immediate and unified follow up of the ruling shows how complex the issue is. On the other hand,

9 Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECL:EU:C:2015:650.

10 Ibid 157.

11 Ibid 153.

12 Ibid. 153.

13 Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems [2020] ECLI:EU:C:2020:559.

the situation in the US is also evolving, and voices in favour of privacy regulation are becoming more perceptible. The framework proposed by Farrell and Newman may again be useful in tracking the interdependences during this new stage of the conflict. It is yet to be seen how the situation develops – but it seems that the NIA will be a valuable tool to track it.

Nevertheless, one may ask whether it is really that easy to abandon the state v. state perspective, especially in cases concerning mass surveillance exercised by one country on the citizens of another. After all, it is the government that remains then the regulator. In transatlantic discussions, all actors involved are coming from similarly democratic systems where, when it comes down to it, both freedom and privacy constitute core values. Would the NIA be equally applicable in assessing clashes in the context of data transfers to countries with demonstrably different privacy and data protection cultures such as China or Russia? Would it be possible to outline similar cross-national networks of privacy- and security-oriented groups of interests with regard to countries that strikingly limit the access of non-state actors to the negotiations? It is conceivable that other lines of demarcation would then have to be drawn.

Of Privacy and Power is a compellingly written book with a clear argument that is convincingly developed throughout the chapters. The authors make a successful attempt to trespass fixed dichotomies and adopt a novel, insightful approach to a subject that has already been discussed so many times. Switching the attention from the simple state v. state divide towards the multisided networks of interdependences responds to the complex challenges of the globalized world. It also allows to include in analyses stakeholders whose impact was previously neglected, if not denied. The perspective proposed by the authors would be of exceptional value for the future examinations of the post-Schrems II negotiations, where a strong influence of transnational non-state actors on both sides cannot be omitted. Likewise, it may be beneficial for observations on ongoing and upcoming debates, such as those around the Digital Single Act in the EU, or discussions in the US on the regulation of the 'Big Tech' companies. Although they both concern domestic affairs, their transnational impact will be unprecedented.

Data Justice and COVID-19: Global Perspectives
by Linnet Taylor, Gargi Sharma, Aaron Martin and Shazade Jameson (eds.)
Meatspace Press 2020; 304 pp
€24.25; Paperback

*Gloria González Fuster**

It has been said before, but, still: what a year. If someone thought that the most challenging issue of 2020 was going to be figuring out how to regulate Artificial Intelligence (AI) in the European Union (EU), or properly assessing the enforcement of the General Data Protection Regulation (GDPR), they got it wrong. We all got it wrong, and we were all eventually shaken, disrupted, worried, and frustrated by a global pandemic that has dramatically impacted all realms of society, including many crucial aspects of our work and daily life.

The Covid-19 outbreak has had – and continues to have - major implications in all policy fields. Technology, cross-cutting among them, has played a key role in shaping such impact since the very start. Technology has served a variety purposes related to public health and beyond. Due to Covid-19, and in a way never experienced before in human history, entire populations started being intermittently almost fully disconnected from what had been until then their normal off-line realities, and confined to online education, online working, online shopping, and online socialising. Eventually, individuals were re-granted certain rights to reconnect with the non-digital, such as the right to move around more or less freely, but conditioned to unprecedented tracking, measuring, and, generally speaking, personal data processing.

Making sense of all this constitutes a challenge in itself. Making sense of it what it is actually happening is even more demanding. *Data Justice and COVID-19: Global Perspectives*[1] is a great resource to help us in this challenging endeavour. Prepared in the context of the Global Data Justice project of the Tilburg Institute for Law, Technology, and Society (TILT), led by Linnet Taylor, it brings together an outstanding

DOI: 10.21552/edpl/2020/4/22

* Research Professor at Vrije Universiteit Brussel (VUB). Co-Director of the Law, Science, Technology and Society (LSTS) Research Group. For correspondence: <Gloria.Gonzalez.Fuster@vub.be>

1 Linnet Taylor, Gargi Sharma, Aaron Martin and Shazade Jameson (eds.), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press, 2020).

group of international researchers, both in terms of quantity and quality; it has among its massive list of contributors some real big names of the ever-expanding world of people studying data-related matters. Written quickly, produced fast, and made available for free in open access with a sleek design, it expresses a genuine vital need to understand how we got here, what happened exactly, where are we going, whether there might be some chance to change direction at some point, and how.

The book is interestingly constructed, built upon a simple trick. It basically consists of 'local dispatches' from around the world, providing glimpses of perspectives from specific countries, separately or jointly (cf. 'Western Balkans', 'Estonia and Finland' are joined), but also of other 'groups' - well, one 'group', that is, the North American Indigenous Peoples. These dispatches are commented upon in nine commentaries, written technically afterwards, but placed nevertheless in the first part of the volume as a sort of introductory reading and thinking guidance.

Data Justice and COVID-19 does not focus on privacy or data protection law. On the contrary, like other initiatives embracing the 'data justice' motto, it is deeply concerned with questioning the viewpoints most commonly adopted to approach data issues, including the privacy and data protection lens. Regularly, if not systematically, it therefore appears to try to push privacy and data protection law out of the centre of the picture, in order to invite for more distinct accounts of other matters otherwise at risk of being relegated to side concerns and nebulous framings.

This does not mean, however, that the volume is unconcerned with privacy and data protection law. Far from it. A number of local dispatches explicitly put forward how the lack of fully applicable data protection laws in their own legal frameworks constituted a major problem to face the Covid-19 outbreak, as well as to deal with policy responses to the crisis. Input on Jordan puts forward concerns about e-wallet platforms being introduced in the absence of strong privacy protection laws.[2] The Chinese contribution evokes how China prioritised, in its response to the epidemic, security over privacy.[3] The Argentinian correspondent laments that Argentinian data protection law has not yet been brought in line with GDPR standards.[4]

We learn that in Ghana there are (limited) hopes that the 2012 Data Protection Act and the Data Protection Commission could, perhaps, reign governmental attempts to control telecommunication systems,[5] but that in Kenya the 2019 Data Protection Act had not yet been operationalised and there was no Data Protection Commissioner as the crisis unfold,[6] creating a problematic gap. It is reported that in Uganda, which also has a 2019 legal instrument, attitudes towards enforcement remain however *'lacklustre'*.[7] The South African dispatch notes the 2013 Protection of Personal Information Act (POPIA) if not yet fully in force, negatively affecting responses to Covid-19-related data initiatives.[8]

Some local reports describe broad public debates around privacy;[9] some echo interventions of national data protection authorities,[10] or illustrate how data protection considerations have in practice modulated, at least, certain data protection practices, for instance on access to data about people's movements.[11] Privacy and data protection concerns pop up in relation to many issues, from the sharing of patient data to legal compliance by Zoom.[12] Julie E. Cohen, reporting on the United States (US), stresses how in her country discussions around Zoom, however, *'deflected attention from the more general default condition of inadequate privacy and data protection'*.[13]

The dispatches chronicle many multifarious configurations of privacy and data protection claims,

2 Raya Sharbain and Anonymous II, 'An e-government strategy that overlooks digital divides', 170-177.

3 Wayne W. Wang (pseudonym), 'Digital collectivism in a global state of emergency', 114-119.

4 Ramiro Alvarez Ugarte, 'Layers of crises: when pandemics meet institutional and economic havoc', 84-89 (esp. 87).

5 Smith Oduro-Marfo, 'Transient crisis, permanent registries', 144-145.

6 Grace Mutung'u, 'Placing all the bets on high technology', 178-183.

7 Daniel Mwesigwa, 'Guerrilla antics, anti-social media, and the war on the pandemic', 270-275.

8 Alison Gillwald, Gabriella Razzano, Andrew Rens, and Anri van der Spuy, 'Protecting mobile user data in contact tracing', 248-253.

9 Ben Wagner, 'Business as usual? Responses to the pandemic', 134-139.

10 Francesca Musiani, 'Apps and submarine cables: reconfiguring technology in a state of urgency' (on France), 126-133.

11 Helen Eenmaa-Dimitrieva, Eneken Tikk, and Mika Kerttunen, 'The politics of a pandemic' (Estonia and Finland), 120-125, esp. 123.

12 Naomi Appelman, Jill Toh, Ronan Ó Fathaigh, and Joris van Hoboken, 'Techno-optimism and solutionism as a crisis response' (on The Netherlands), 190-197.

13 Julie E. Cohen, Capitalising on crisis, 284-291, esp. 286.

from civil society and academics actively calling on a government to consider applying the recommendations of the European Data Protection Board (EDPB),[14] to national data protection authorities being perceived as being paradoxically too supportive of 'contact-tracing' apps in contrast with a reluctant population with persistent privacy concerns.[15] Some authors actively mobilise in their analysis of local Covid-19 related developments the reading of data protection notices,[16] or discuss privacy impact assessments.[17] Where data protection laws are in place they shall not, however, be taken for granted – especially not in times of crisis. That is a key message from the analysis of the situation in Hungary,[18] where data protection rights stand out as direct targets of a deterioration of democracy accelerated by the virus.

The 'local dispatches' represent probably the book's most significant contribution to the state of our knowledge on data issues around the Covid-19 outbreak, giving substance to the 'global' reference in the book's subtitle, and illustrating the fragmentation of experiences and understandings that these times are critically exacerbating. It might not easy to draw comparisons between countries, but peculiarities emerge in interesting ways. There are, of course, no winners: only the Norwegian correspondent felt somehow entitled to describe her country as '*a COVID-19 success story*',[19] before nonetheless describing many tensions around data protection and human rights. There is unfortunately no dispatch on the EU, or any substantive transversal reflection about the place of the EU amidst all these developments, despite the fact that there is certainly much to say about how it affected - and was affected by – the described evolving dynamics of state and corporate power.

The horizontal commentaries have the difficult task of situating all reports highlighting trends, and delineating a series of broader pictures, without sounding excessively reductive. Their contributions are not particularly well-served by the book designers, who, privileging aesthetics in detriment of basic rules of typography and politeness towards hard-working academics with tired eyes, dropped these texts in white letters against a deep grey background. The commentaries' authors were also not helped by the fact most of them get to offer their own broader picture from a rather similar standpoint, meaning that, in the end, the United Kingdom (UK) is still in the very centre of many authors' minds, BBC News the unquestioned soundtrack,[20] and, in sum, and to to paraphrase Protagoras, of all things Covid-19-related the measure is Dominic Cummings.

Privacy surfaces – again - in almost all of these horizontal commentaries.[21] Vidushi Marda contests the validity of any privacy versus health trade-offs,[22] referring to a '*nefarious*' false dichotomy.[23] Os Keyes stresses the importance of visibility that some privacy discussions do not fully integrate.[24] Lilian Edwards describes how privacy has been perceived as a condition for adoption of 'contact-tracing' apps,[25] and Sean Martin McDonald refers to debates opposing data architecture choices to privacy rights.[26] Michael Veale provides a very interesting account on the proliferation of 'contact-tracing' apps in Europe,[27] in which reference is made to attempts to mis-use of the (naïf?) embracing by a large part of the privacy community of certain technological solutions,[28] the (unstoppable?) power of Google and Apple, and some (too late, too weak, too desperate?) attempts to counter such power by European sovereign governments, all somehow connected to the '*strange*' (in his own words) assumptions in which appear to be

14 Rob Kitchin, 'A marginal contribution to the pandemic response?' (on Ireland), 154-159.

15 Liliana Arroyo Moliner and Enric Luján, 'Political incoordination and technological solutionism amidst the lack of tests' (on Spain), 262-269.

16 Magda Brewczyńska, 'Policing quarantine via app' (on Poland), 232-239.

17 Fleur Johns, 'Counting, countering and claiming the pandemic: digital practices, players, policies' (on Australia), 90-99.

18 István Böröcz, 'Suspending rights and freedoms in a pandemic-induced state of danger', 146-153.

19 Kristin Bergtora Sandvik, 'Smittestopp: the rise and fall of a technofix', 210-223.

20 Anonymous I, 'Reining in humanitarian technology', 70-75.

21 Sometimes indirectly; for instance Dragana Kaurin notes that even before discussing privacy concerns of 'contact-tracing' apps it is necessary to ask if the approach is the right approach (cf. 'The dangers of digital contact tracing: lessons from the HIV pandemic', 64-69).

22 Vidushi Marda, 'Papering over the cracks: on privacy versus health', 28-33.

23 ibid. 33.

24 Os Keyes, 'Who counts? Contact tracing and the perils of privacy', 58-63.

25 Lilian Edwards 'Apps, politics, and power: protecting rights with legal and software code', 40-49.

26 Sean Martin McDonald, 'Technology theatre and seizure', pp. 20-27.

27 Michael Veale, 'Sovereignty, privacy and contact tracing protocols', pp. 34-39.

28 ibid. 36

grounded the work of the designers of 'privacy-preserving technologies'.[29]

All in all, *Data Justice and COVID-19* is an impressive piece of collective work, covering much more than privacy and data protection law issues, but still indispensable for privacy and data protection law scholars. It is tempting to say it will become a reference for all future research about what happened with (and to) data at the beginning of the Covid-19 global crisis. Let's hope it becomes, first, a basic read to think and discuss what is to happen now.

29 ibid. 39.