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.

Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis
By Maria Grazia Porcedda
Hart 2023, 344 pp.
£90.00; Hardback

*Luca Tosoni**

Is it possible to achieve cybersecurity while safeguarding the fundamental rights to privacy and data protection? This book is an elegant attempt to answer this complex question in a European Union (EU) law context.

At a juncture when cybersecurity is gaining normative and practical prominence across the globe, and the EU is revamping its cybersecurity legal framework, Porcedda's book offers a welcome compass to navigate this intricate legal area and strike a fair balance between competing rights and interests. It should be on the reading list of those scholars, practitioners, and lawmakers who strive to investigate, design and implement measures that provide a high level of cybersecurity while ensuring full compliance with fundamental rights.

While there is abundance of literature on cybersecurity, privacy and data protection as separate regulatory objectives under EU law, there is more limited literature on their interplay.[1] Therefore, the book helps to fill gaps in the literature, and provides a much-needed analysis of how these three objectives are and can be reconciled across different policy areas.

In the volume, the author explores the connections, complexities and tensions that exist among cybersecurity, privacy and data protection, including as they emerge from a wide range of EU legal instruments, such as, among others, the General Data Protection Regulation (GDPR), the Directive on Security of Network and Information Systems (NIS Directive), e-evidence and cybercrime legislation. The analysis offered combines legal, policy and technological perspectives, and is enriched by numerous practical examples, which help the reader to follow the author's reasoning as it unfolds.

The book is divided into two parts. The first part unpacks the notions of cybersecurity, privacy and data protection, as well as their relationship. In this part, insights are drawn from different disciplines, such as informatics, international relations, political science and law, which make Porcedda's work partly interdisciplinary in nature.[2] While the author's conclusion that cybersecurity, privacy and data protection can at once clash and complement each other is hardly surprising for anyone familiar with the field, the analytical framework that Porcedda proposes to investigate how these can be reconciled is partly innovative and requires readers to familiarize themselves with it before moving on to the second part of the book.

The work's second part illustrates how cybersecurity, privacy and data protection are, or can be, balanced in practice across several key EU policy areas, including the digital single market, the area of freedom, security and justice, the common foreign and security policy, the common security and defence policy and the common commercial policy. In essence, most of the areas where cybersecurity issues are likely to arise and where the EU enjoys some legislative competences are covered.

DOI: 10.21552/edpl/2023/4/16

* Luca Tosoni is Associate Professor at Inland Norway University of Applied Sciences, and Specialist Director at the Norwegian Data Protection Authority. For correspondence: <luca.tosoni@datatilsynet.no>.

[1] See eg, G González Fuster and C Jasmontaite, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights' in M Christen et al (eds), *The Ethics of Cybersecurity* (Springer 2020) 97; A Mantelero and G Vaciago, 'Reconciling Data Protection and Cybersecurity: An Operational Approach for Business Sector' in R Senigaglia et al (eds), *Privacy and Data Protection in Software Services* (Springer 2022) 97.

[2] BMJ van Klink and HS Taekema, 'On the Border: Limits and Possibilities of Interdisciplinary Research' in BMJ van Klink and HS Taekema (eds), *Law and Method: Interdisciplinary Research into Law* (Mohr Siebeck 2011) 7.

It is in part two of the book where the most significant contribution of the author lies. Here Porcedda ventures into a rather detailed assessment of how cybersecurity, privacy and data protection are to be reconciled in numerous concrete policies and legal instruments. This includes an analysis of regulatory measures that are high on the agenda of policy makers, although they present particularly acute inherent tensions between cybersecurity, privacy and data protection, such as the scanning of electronic communications in the fight against child sexual abuse online,[3] or the use of deep packet inspection in the fight against cybercrime.[4] Therefore, researchers, policy makers, digital rights activists and lawyers involved in the design and implementation of EU digital policies may take particular interest in the analysis presented in this part.

Given the complexity of the subject matter of the book, it was understandably not possible for the author to leave no stone unturned regarding the existing interconnections between cybersecurity, privacy, and data protection. For example, a few issues of high practical significance—such as whether and to what extent the GDPR provides an adequate legal basis to justify the processing of personal data for a wide range of cybersecurity purposes,[5] or how to reconcile privacy and cybersecurity in internet governance[6]—have not or only sparsely been addressed. Moreover, the emerging discourse on the recognition of a fundamental right to cybersecurity[7]—which may need to be balanced with the rights to privacy and data protection, should cybersecurity attain fundamental right status of its own[8]—has not been given much attention.[9] Nonetheless, the book provides a solid building block for further research in the field.

At the end of the volume, Porcedda outlines a few future challenges and research trajectories that may stem from her work. In particular, she highlights the need to take into account that the ongoing technological, social and policy developments may 'have an impact on much more than the triad [analysed in her book]. At stake are not just cybersecurity, privacy and data protection, but the survival of democratic orders and the flourishing of human nature as we know it'.[10] To this it may be added that cybersecurity is becoming increasingly important to ensure the enjoyment of *all* fundamental rights online and offline.[11] Therefore, there is a need for future research that will leverage off insights drawn from existing scholarship, including Porcedda's research, to explore how a broader range of fundamental rights may be reconciled with cybersecurity aspirations.

In conclusion, *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis* is a highly commendable work and provides a timely analysis of the elements to be taken into account when balancing partially opposing interests and rights in a digital context. It is a laudable attempt to move beyond the zero-sum game attitude that too often characterizes the discourse on the relationship between cybersecurity, privacy and data protection.

[3] See T Quintel, 'The Commission Proposal on Combatting Child Sexual Abuse - Confidentiality of Communications at Risk?' (2022) 8 European Data Protection Law Review 262; EDPB-EDPS, Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (28 July 2022).

[4] S Stalla-Bourdillon et al, 'From porn to cybersecurity passing by copyright: How mass surveillance technologies are gaining legitimacy … The case of deep packet inspection technologies' (2014) 30(6) Computer Law & Security Review 670.

[5] Cf eg, Case C-252/21 *Meta Platforms and Others* [2023] ECLI:EU:C:2023:537, paras 119-121.

[6] See eg, M Muller and M Chango, 'Disrupting Global Governance: The Internet Whois Service, ICANN, and Privacy' (2008) 5(3) Journal of Information Technology & Politics 303; J Kulesza, 'Balancing Privacy and Security in a Multistakeholder Environment. ICANN, WHOIS and GDPR' (2018) 3 The Visio Journal 49.

[7] See eg, V Papakonstantinou, 'Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?' (2022) 44 Computer Law & Security Review 10565; I Pernice, 'Global cybersecurity governance: A constitutionalist analysis' (2018) 7(1) Global Constitutionalism 112; I Kilovaty, 'An Extraterritorial Human Right to Cybersecurity' (2020) 10(1) Notre Dame Journal of International & Comparative Law 35.

[8] The elevation of cybersecurity to a fundamental right would place it on an equal footing with other fundamental rights, thus changing the nature of the balancing act. See I Walden, '"The Sky is Falling!" – Responses to the "Going Dark" problem' (2018) 34 Computer Law & Security Review 34, 907.

[9] However, the author does acknowledge the existence of this discourse. See MG Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis* (Hart 2023) 13.

[10] Ibid, 269.

[11] Human Rights Council, Resolution 47/16 on the promotion, protection and enjoyment of human rights on the Internet, UN Doc A/HRC/RES/47/16 (26 July 2021).