scripted

Volume 21, December 2024

Book review: *Vulnerability and Data Protection Law*

Gianclaudio Malgieri
Oxford University Press 2023. 304 pages.
ISBN 9780192870339. £90.

*Reviewed by Mona Winau**

DOI: 10.2218/scrip.210024.99

* Project Researcher, KASTEL Research Labs, Karlsruhe Institute of Technology, Germany, mona.winau@kit.edu.

The processing of personal data creates power imbalances to the detriment of data subjects; these grow with the advancing possibilities of algorithm-based personalisation to predict and influence behaviour. While data protection law aims to ensure fairness in such unequal relationships, the awareness of personal conditions and particular circumstances that must be taken into account for creating a fair balance has so far only poorly been reflected. Addressing this shortcoming, *Gianclaudio Malgieri* develops a vulnerability-based interpretation of data protection law as a heuristic tool to enhance fairness in power imbalanced relationships. Taking up the bioethical theory of layered vulnerability by *Florencia Luna*,[1] he determines the notions of an "average" data subject and a "vulnerable" data subject under GDPR and proposes an individual-centric approach to assessing risks to fundamental rights and freedoms of natural persons by determining sources of vulnerability to which mitigation measures should be tailored.

Starting with an introductory chapter, the need for interpretation of data protection law taking into account layers of vulnerabilities affecting data subjects and not only roughly defined groups of vulnerable persons like children or elderly is set out. The following chapters 2, 3 and 4 determine the notion of the data subject, the vulnerable person, and the vulnerable data subject. Based on this, chapters 5, 6 and 7 provide for an individual-centric interpretation and implementation of data protection principles, rights of data subjects as well as obligations of controllers and the data protection impact assessment. Chapter 8 deals with limitations of the proposed interpretation and ways to overcome them

[1] Florencia Luna, 'Eludicating the Concept of Vulnerability: Layers Not Labels' (2009) 2 International Journal of Feminist Approaches to Bioethics 121 and 'Identifying and Evaluating Layers of Vulnerability – a Way Forward' (2019) 19 Developing World Bioethics 86.

including the recommendation for specifying vulnerability *de lege ferenda*. Finally, the main hypotheses are summarised in chapter 9.

Both the clear structure of the book and the reader-friendly concept of an introductory section at the beginning and a concluding section at the end of each chapter make it easy to follow the train of thought and allow for a selective reading of certain chapters. Well-articulated hypotheses, their clear reasoning, and contextualisation lead rationally to the author's main demand for an individual-centric interpretation of data protection law, tailored to layers of vulnerabilities of data subjects.

Much appreciated is the determination of the notion of the data subject and the vulnerable data subject, considering both are not defined under GDPR. Through a normative interpretation of the notion, the data subject would be dynamic as it refers to identifiability which is a relational and context-dependent requirement. At the same time, it would be general and universal as it would cover all living natural persons. Based on an evaluative interpretation and a comparison with consumer protection law, the data subject would be considered as rational and well informed. The following criticism of this concept of the "average" consumer or data subject as being mostly out of touch with reality is clearly justified. Furthermore, the finding that, due to the GDPR's regulatory concept which does not entirely rely on consent and the acknowledgement of the actual non-informed data subject by the CJEU, GDPR allows for a hybrid approach that recognises not only the average data subject but also the data subject who is considered vulnerable in certain contexts, is reasonable. Here, it would also have been rewarding to analyse the GDPR's dual objective including the protection of fundamental rights and freedoms as individual rights and in the sense of common values. Dignity as the basis of fundamental rights in Europe, which requires protection against individual vulnerabilities, could have also been referred to as this is considered later.

With the transfer of the concept of layered vulnerability, based on a theoretical consideration of particularistic and universal understandings of vulnerability, and an analysis of the understanding of vulnerable persons in the ECtHR jurisprudence and under EU secondary law, the reader's awareness is raised for the contextuality and relative nature of persons' vulnerability as well as their different sources. The main hypothesis that vulnerability of data subjects would need to be determined by means of specific power imbalances in their relation to the controller that cause a higher risk to their fundamental rights and freedoms is consequently followed from the preceding understanding and an analysis of the notion of vulnerability under data protection law. A key finding from that is furthermore that data subjects' vulnerability could manifest itself in two different states: during the data processing or as an outcome of the data processing.

The consideration of data protection principles, rights and duties under the perspective of personal vulnerabilities substantiate how GDPR can be interpreted individual-centric. Not new in its purview, but appreciated for its clarity, is the statement that due to the principles of fairness and lawfulness, a processing of personal data could not be based on consent in the event the data subject's vulnerability that affects the decision making. In the case of vulnerability as an overweighing risk for fundamental rights and freedoms which cannot be mitigated, it could also not be based on a legitimate interest. The purpose of the proposed concept and what it means for the application of data protection law becomes clearer in chapter 7, where the DPIA is used to specify how GDPR provisions can mitigate negative impacts of data processing on vulnerable data subjects. However, while it is argued that an analysis of the severity and likelihood of risks could be based on an analysis of layers of vulnerability of the data subject, it remains unresolved to what extent and how different vulnerability factors would cause a high risk for the interference of

fundamental rights and freedoms, and respectively to what extent tailored mitigation measures must be implemented to reach an acceptable risk level.

Persuasively, limitations of the approach are outlined, and potential criticism is addressed in chapter 8. It becomes particularly clear herein that the proposed concept is individual-centric but relies on structural and situational analyses of vulnerability factors. This means a controller should be aware of situations in which he (most likely) processes data of vulnerable data subjects and address these but not analyse the individual vulnerabilities of specific (groups of) data subjects for the sake of individually tailored mitigation measures. As it is outlined, this follows from data protection law and the logic of the concept itself without any doubt. However, it remains unclear whether in situations where there are (likely to be) layers of vulnerability, tailored risk mitigation measures must apply preventively as a general standard and to all data subjects, including those who are not vulnerable, and how to proceed in situations where there are different vulnerability layers requiring different mitigation measures for certain (groups of) data subjects.

De lege ferenda, a general definition of vulnerability in the law, complemented by constantly updated guidelines that concretise vulnerability factors and suitable mitigation measures, is argued for. Here, a concrete proposal on how the notion of vulnerability could be defined in data protection law, based on the previously outlined understanding of the vulnerable data subject, would have been desirable.

Overall, *Malgieri* presents an innovative understanding of data protection law that addresses essential problems such as the ineffectiveness of consent in practice and tick-box-compliance in the context of risk mitigation measures, and thus provides a precious contribution to the academic debate. The foundations of the legal analysis are as broad as relevant and include theoretical approaches to vulnerability in neighbouring sciences; EU and member state law regarding

data protection, consumer protection and other relevant areas such as research regulations and clinical trials; interpretations of data protection law by EU bodies, national authorities, and academia as well as relevant EU law jurisprudence. Despite the complexity and abstractness of the subject matter, the proposed concept is illustrated with examples, making it tangible for its application. This book is recommended for anyone who is academically interested in data protection law and has the potential to also influence its interpretation and application in practice.