# Book review: Gianclaudio Malgieri, Vulnerability and Data Protection Law. 1st edn. Oxford University Press, 2023

Faisal, Kamrul

Juridiska Föreningen i Finland
2024-04-18

Faisal, K 2024, 'Book review: Gianclaudio Malgieri, Vulnerability and Data Protection Law. 1st edn. Oxford University Press, 2023', Tidskrift utgiven av Juridiska föreningen i Finland, vol. 160, no. 1-2, pp. 99-109. < https://www.edilex.fi/jft/1001150004 >

http://hdl.handle.net/10138/575055

unspecified
publishedVersion

JFT 1–2/2024 s. 99–109

LITTERATUR

Bokrecension

# Gianclaudio Malgieri, Vulnerability and Data Protection Law. 1st edn. Oxford University Press, 2023, 304 pages.

## 1 Summary of the book

The purpose of writing this book review is to critically analyze the content, structure, and overall contribution of the study *Vulnerability and Data Protection Law*,[1] authored by Gianclaudio Malgieri. Overall, it is a must-read book for anyone who interacts with the digital environment since the book enhances current understandings of the inequalities, power dynamics, policy developments, exploitation prevention, and so forth, impacting the European Union's (EU) data protection laws. In his book, Malgieri (re)conceptualizes "vulnerability" in association with humans (he uses the collective term "vulnerable natural persons," also referring to them as "vulnerable data subjects") under the General Data Protection Regulation (GDPR). Therefore, I will also use the terms interchangeably throughout this review. Malgieri begins the book by outlining the rationale for researching vulnerability in relation to the GDPR (chapter 1). The book has two main objectives: first, it (re)conceptualizes the notion of vulnerable data subjects (chapters 2–4), and second it makes an argument for strengthening the protection of vulnerable data subjects under the GDPR in a digital context (chapters 5–7). Lastly (in chapter 8), the book addresses some criticisms. The use of normative and descriptive research methods helped the author attain his objectives convincingly and coherently.[2]

Malgieri chose to research vulnerability to help readers understand the necessity of studying vulnerability issues under the GDPR. Emerging data processing technologies have put humans in a power-imbalance relationship between the data subjects and the controllers, in which controllers occupy the superior position and data subjects the inferior one. Empirical data shows that the superior position holders (the controllers) may pose a risk to data subjects' rights and freedoms in relation to their personal data protection and other rights in a way that may be inconsistent with certain GDPR provisions.[3] Keeping that in mind, recognizing data subjects as vulnerable and in need

---

[1] Gianclaudio Malgieri, Vulnerability and Data Protection Law (Oxford: Oxford University Press, 2023).

[2] Gianclaudio Malgieri, "The Reasons for Research on Data Subjects," in Vulnerability and Data Protection Law, 7.

[3] Malgieri, "The Reasons for Research," 1.

of protection may help correct the imbalance by imposing additional obligations on the controllers, thereby forcing them not to put vulnerable individuals at such risk by exploiting their vulnerabilities.[4]

The GDPR does not define the concept of "vulnerability" at all. Rather, it uses the phrase "vulnerable natural persons" once in Recital 75, categorizing children as part of that group.[5] Malgieri analyses the term "natural person" in alignment with the concept of "data subject," which the GDPR only implicitly suggests. The definition of data subject reveals certain elements related to vulnerability, namely that data subject(s) are natural persons who are identified or identifiable through any information related to them. According to the definition, insofar as a piece of information identifies or creates the possibility of identifying a human being, he/she is considered a data subject for the GDPR. The data subject(s) can be an individual and/or group.[6] Similarly, vulnerable natural persons or data subjects can be considered on an individual and/or group-based level (e.g., children).[7] The notion of data subject(s) does not help us much in conceptualizing vulnerable data subjects. To do this, the author takes the reader beyond the scope of the EU's data protection law.

Primary laws, such as the Treaty on the European Union (TEU) or the Treaty on the Functioning of the European Union (TFEU), do not contain any notion of vulnerability.[8] The author conceptualizes vulnerability under the GDPR by drawing an analogy from specific European secondary laws, mainly on consumer protection,[9] human subjects in clinical trials, pertinent case laws of the EU, and disparate national practices.

A classical definition of vulnerability may have originated from the Latin word *vulnus*, meaning fragility, wound, or harm.[10] Refugees, racial and ethnic minorities, disabled people, and others comprise traditional vulnerable human groups who demonstrate vulnerability based on their unique situations.[11] The GDPR understands vulnerability as a fact-based situation in which data subjects remain at risk of harm

4 Malgieri, "The Reasons for Research," 2.

5 Malgieri, "The Reasons for Research".

6 Malgieri, "The Reasons for Research," 26.

7 Malgieri, "The Reasons for Research," 6–7.

8 Gianclaudio Malgieri, "Who Is the Vulnerable Individual?" in Vulnerability and Data Protection Law, 61.

9 Malgieri, "The Reasons for Research," 2; Malgieri, "Who Is the Vulnerable Individual?" 8.

10 Catriona Mackenzie, Wendy Rogers, and Susan Dodds, "Introduction: What Is Vulnerability, and Why Does It Matter for Moral Theory?" in Vulnerability: New Essays in Ethics and Feminist Philosophy, ed. Catriona Mackenzie, Wendy Rogers, and Susan Dodds (Oxford: Oxford University Press, 2013); Gianclaudio Malgieri and Jędrzej Niklas, "Vulnerable Data Subjects" Computer Law and Security Review 37 (2020): 1; Malgieri, "Who Is the Vulnerable Individual?".

11 Malgieri, "Who Is the Vulnerable Individual?" 49.

with respect to their right to privacy and personal data protection due to the existence of a power-imbalance relationship between data subjects and controllers,[12] which may impair the ability to control one's data.[13] Superior and inferior position holders possess different sets of powers. For example, controllers possess market powers, while data subjects possess the power of knowledge,[14] such as awareness, privacy literacy, resilience, or cognitive decision-making capacity.[15] In the digital context, controllers' power may allow them to reduce data subjects' power quite easily by prompting them to accept new requests that would compromise their data.[16] For instance, controllers may exploit data subjects' vulnerability by collecting information from vulnerable data subjects for targeted advertisement purposes,[17] which may in turn put them at great risk in terms of the fundamental rights and freedoms related to human dignity,[18] privacy, and data protection laws, as well as freedom of speech, prohibitions against discrimination, the right to liberty, and the freedom to conduct business.[19] Here, three factors contribute to creating vulnerability: data subjects' characteristics, controller power, and the mechanism for causing vulnerability.[20]

So, how can vulnerable data subjects be identified? It is necessary to analyze the existing power structures when assessing vulnerability.[21] In outlining various typologies, Malgieri identifies that humans can be both universally (everyone is vulnerable) and particularly (some people are more vulnerable than others) vulnerable. Though both types of vulnerability pose risks to fundamental rights and freedoms, the GDPR protects "particularly vulnerable" data subjects, making vulnerability legally relevant or meaningful. This helps experts identify the existence of a "significant power imbalance," rather than just identify anyone as vulnerable (considering everyone vulnerable

[12] Malgieri, "Who Is the Vulnerable Individual?" 51.

[13] Malgieri, "Who Is the Vulnerable Individual?"; Gianclaudio Malgieri, "The Vulnerable Data Subject in the GDPR," in Vulnerability and Data Protection Law.

[14] Malgieri, "Who Is the Vulnerable Individual?" 54.

[15] Malgieri, "The Reasons for Research," 26.

[16] Malgieri, "Who Is the Vulnerable Individual?" 54.

[17] Gianclaudio Malgieri, "The Limitations and the Alternatives of a Vulnerability-Based Interpretation of the GDPR," in Vulnerability and Data Protection Law, 225.

[18] Malgieri, "Who Is the Vulnerable Individual?" 57.

[19] Malgieri, "The Vulnerable Data Subject in the GDPR,"; Gianclaudio Malgieri, "Assessing (and Mitigating) Layers of Data Subjects' Vulnerability: Using the DPIA as a Model," in Vulnerability and Data Protection Law.

[20] Gianclaudio Malgieri, "Conclusions: The Layers of Data Subject's Vulnerability and the Way Ahead," in Vulnerability and Data Protection Law, 232.

[21] Malgieri, "Who Is the Vulnerable Individual?" 74.

makes the vulnerability approach meaningless and nebulous) data subjects.[22] Children and the mentally ill may by default be affected by significant power-imbalance relationships, which makes them vulnerable data subjects under the GDPR. Additionally, groups like patients and employees may also be subject to significant power-imbalance relationships or may be considered vulnerable data subjects under the GDPR depending on the significant power-imbalance contexts.[23] So, how is it possible to identify vulnerable data subjects among adults by analyzing existing power structures?

Luna's layered approach helps in this regard,[24] since it considers the complex personal characteristics of data subjects based on the risks specified by the GDPR.[25] For example, layers may be associated with age, cognitive circumstances (such as whether data subjects are in a position to freely give specific, explicit, and unambiguous consent), awareness, and different categories of personal data related to its nature, context, scope, and data protection rights.

Overall, though the implied GDPR definition of a data subject does not indicate the possibility of different types of data subjects,[26] a teleological interpretation of the relevant GDPR provisions reveals that there may be average and vulnerable data subjects.[27] An average data subject may be "reasonably well-informed and observant and circumspect," which makes vulnerable data subjects different from them.[28] Personal variables seem to be responsible for bringing such typologies to light.[29] Therefore, the concept of data subject(s) should be dynamic and not static.[30] Vulnerable data subjects receive greater protection compared to their counterparts, the average data subject, since processing vulnerable people's data may require controllers to comply with additional requirements to protect them from possible harm related to their rights and freedoms.[31]

Significant power-imbalance relationships and a high level of risk to one's rights and freedoms are the two most important elements of any legally relevant vulnerable situation. To assess significant power imbalances, the author suggests looking into two components: first, interferences with fundamental rights and freedoms, and second, the

[22] Malgieri, "The Vulnerable Data Subject," 95.

[23] Malgieri, "The Vulnerable Data Subject," 80.

[24] Malgieri, "Conclusions," 231.

[25] Malgieri, "The Vulnerable Data Subject in the GDPR," 90.

[26] Malgieri, "Conclusions," 228.

[27] Malgieri, "The Reasons for Research," 16.

[28] Malgieri, "The Reasons for Research," 27.

[29] Malgieri, "Conclusions," 228.

[30] Malgieri, "Conclusions," 231.

[31] Malgieri, "Conclusions," 228.

severity of the effect produced by the interferences.[32] Moreover, the risks may include subjective and objective perceptions of harm and can likewise include the exploitation of effect-based (interferes with other fundamental rights) and processing-based vulnerability (interferes with the right to privacy and personal data protection).[33]

When describing the protections that vulnerable data subjects receive under the GDPR, controllers are responsible for analyzing the existence of any such vulnerability proactively and acting accordingly because they bear the responsibility for making data subjects vulnerable. As such, controllers may be required to devise a three-step test to mitigate the power imbalance as well as related vulnerabilities. It should assess whether controllers specifically target vulnerable individuals, how data processing techniques use knowledge about individual vulnerabilities, and whether controllers believe that they have the power to, for example, exert control over data processing techniques, the capacity for powerful data mining, or make other data extensively available.[34] For instance, if a healthcare authority provides a service for a patient, then they must deploy vulnerability-specific settings. Certain GDPR provisions, including data processing principles and rights, prevent controllers from processing personal data in a significant power-imbalance relationship in a carte blanch manner. For example, processing data based on a general power imbalance may violate the GDPR's principles regarding lawfulness, fairness, and transparency.[35] Such provisions collectively, according to the author, guide the controllers to adopt a vulnerability-aware enforcement mechanism. In this way, the GDPR aims to limit controller behavior and protect vulnerable data subjects.

Moreover, the GDPR makes controllers responsible for conducting a data protection impact assessment (DPIA) before processing such data.[36] Different layers of risk comprise different layers of vulnerability, making it necessary to analyze different elements of risk, according to Art. 35 of the GDPR.[37] If there is no way of preventing how controllers exploit people's vulnerabilities, then the controller should avoid processing the data,[38] which may be unlikely in the case of an average data subject.

Overall, vulnerability is a "heuristic tool" used to interpret the system of rights, duties, and safeguards under the GDPR, which makes it possible to reconceptualize

[32] Malgieri, "The Limitations and the Alternatives," 201.

[33] Malgieri, "Conclusions," 234.

[34] Malgieri, "The Limitations and the Alternatives," 225.

[35] Malgieri, "The Reasons for Research," 1.

[36] Gianclaudio Malgieri, "Data Protection Principles and Vulnerable Data Subjects," in Vulnerability and Data Protection Law, 130.

[37] Malgieri, "Assessing (and Mitigating) Layers," 186.

[38] Malgieri, "Assessing (and Mitigating) Layers".

the risk-based approach surrounding data subjects. Analyzing vulnerability means analyzing the risks.[39] The DPIA provided by the GDPR provides such a tool for analyzing vulnerability.

At the end of the study (chapter 8), Malgieri analyzes some of the criticisms of vulnerable-based interpretations. This approach, in my opinion, aids readers in exploring and understanding various viewpoints on vulnerability, helps hone the book's arguments, and keeps lawyers up to date on the constantly changing legal landscape.

## 2 Analysis of content

### *2.1 Main contributions and strengths*

The key contribution of this book is that the author provides an innovative way of thinking about the concept of vulnerable data subjects under the GDPR. It is a response to the fact that contemporary technological developments lack vulnerability-specific privacy tools to protect vulnerable people in power-imbalance relationships.[40] They require specific privacy protection mechanisms,[41] which the controllers may deploy to provide so-called vulnerable data subjects with extended protection.[42]

The strategy of (re)conceptualizing the vulnerability concept in combination with an understanding of significant power imbalances helps address the unique challenges and risks that vulnerable data subjects often face in digital settings. While establishing procedural norms concerning the exercise of the fundamental right to personal data protection, the GDPR also provides guidelines for the control of personal data in the hands of the respective data subjects through data protection rights and so forth.[43] However, in cases involving vulnerable data subjects, the subjects in question may have less control over their data due to mental, physical, socioeconomic, and other challenges,[44] since they lack the power to protect their interests,[45] which creates a

[39] Malgieri, "Conclusions," 234.

[40] Tommaso Crepax et al., "Information Technologies Exposing Children to Privacy Risks: Domains and Children-Specific Technical Controls," Computer Standards and Interfaces 82, no. 1 (2022): 1.

[41] Tommaso Crepax et al., "Information Technologies," 2.

[42] Stanislaw Piasecki and Jiahong Chen, "Complying with the GDPR When Vulnerable People Use Smart Devices," International Data Privacy Law 12, no. 113 (2022): 130.

[43] Alessandro Mantelero, Beyond Data, Human Rights, Ethical and Social Impact Assessment in AI (Berlin, Heidelberg: Springer-Verlag, 2022) 10.

[44] Piasecki and Chen, "Complying with the GDPR," 114–115.

[45] Florencia Luna, "Identifying and Evaluating Layers of Vulnerability – a Way Forward," Developing World Bioethics 19, no. 86 (2019): 89.

higher risk when it comes to ensuring their rights.[46] In such situations, controllers may not rely on certain existing laws, such as consent, since vulnerable data subjects may not fully understand what is at stake when giving their legally valid (freely given, explicit, informed, and unambiguous) consent.[47] For example, it may not always be permissible for employers to obtain employee consent before processing their data. Thus, controllers' power outweighs the power of data subjects considerably, and theories concerning vulnerable data subjects assist researchers in analyzing different power-imbalance relationships, such as those between employer and employee, government and citizens, online platforms and users, healthcare providers and patients, service providers and consumers, and researchers and research participants.[48] In such situations, controllers must be prevented from exploiting human vulnerability (also known as data necropolitics[49]).

While providing a high-risk-based approach to protecting vulnerable people's data,[50] the GDPR also imposes additional responsibilities on the controller(s). Such risks may arise when processing any type of personal information, such as basic personal data like name, mailing address, email address, location, payment card, sensitive personal data,[51] and data concerning criminal convictions and offenses.[52] Since the GDPR provides extended protection to vulnerable people against physical, material, and non-material damages, we must develop a vulnerability-aware data processing eco-

[46] Recital 69, REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) 2022 (Official Journal of the European Union), 1.

[47] Kamrul Faisal, "Decoding Vulnerability within the GDPR" (CiTiP Blog, 2024), <https://www.law.kuleuven.be/citip/blog/decoding-vulnerability-within-the-gdpr/> (accessed February 20, 2024).

[48] Faisal, "Decoding Vulnerability".

[49] Antonio Pele and Caitlin Mulholland, "On Facial Recognition, Regulation, and 'Data Necropolitics'," Indiana Journal of Global Legal Studies 30 (2023): 173; REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[50] Recital 75, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) 2016, 1–119.

[51] Article 9 of the GDPR states that any personal information revealing racial and ethnic origin, political opinions, religious beliefs, genetic or biometric information, health data, information concerning a person's sex life and sexual orientation, and so forth are categorized as special categories of personal data. According to Recital 10, special categories of personal data are also known as sensitive personal data.

[52] According to Recital 19 of the GDPR, data on criminal convictions and offenses include, but are not limited to, information concerning the prevention, investigation, detection, or prosecution of criminal offenses, execution of criminal penalties, safeguarding against and preventing threats to public security, and free movement of such data.

system.[53] As a tool, controllers may follow the DPIA mechanism outlined in the GDPR to demonstrate compliance with the GDPR.[54] Article 29 Data Protection Working Party (predecessor to the European Data Protection Board), provides comprehensive guidelines for conducting DPIA before processing vulnerable people's data, which include describing all processing activities and assessing the necessity for, proportionality of, and risks to people's rights and freedoms as well as measures for addressing those risks, proper documentation, and ways to monitor and review the measures.[55]

Overall, this is a way of empowering vulnerable data subjects by imposing additional obligations on the controllers, one that respects various aspects of vulnerability. The impacts of this approach on data subjects are not limited to the present day only; they also extend into the future by seeking to address and remedy new and novel situations. For example, emerging technologies like AI and biometrics, international data transfers, children's online privacy, smart city surveillance technologies,[56] and crisis and emergency response situations, such as COVID-19, require careful examination to prevent potential harm. That is why safeguarding data subjects based on vulnerability requires a serious commitment on behalf of the controllers, ensuring that they implement robust safeguards that prioritize data processing principles, data protection rights, and data subjects' well-being in a digital context.

### *2.2 A way forward*

Despite contributing greatly to scholarship on vulnerable data subject(s), the book leaves some questions unanswered. First, children may, for instance, always be considered vulnerable data subjects since they only grow up gradually and may remain in a significant power-imbalance relationship for many years.[57] They also receive exclusive and more extensive protection under the GDPR.[58] For example, the GDPR notes

[53] Stanislaw Piasecki, "Expert Perspectives on GDPR Compliance in the Context of Smart Homes and Vulnerable Persons," Information and Communications Technology Law 32 (2023): 385, 413, <https://doi.org/10.1080/13600834.2023.2231326>.

[54] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" in relation to Regulation 2016/679 2017 (Article 29 Working Party), 1, 9.

[55] Regulation 2016/679 2017 (Article 29 Working Party), 16.

[56] Kamrul Faisal, "Applying the Purpose Limitation Principle in Smart-City Data-Processing Practices: A European Data Protection Law Perspective," Communication Law and Policy 28 (2023): 67, <https://doi.org/10.1080/10811680.2023.2180266>.

[57] Opinion 2/2009 on the protection of children's personal data (general guidelines and the special case of schools) (2009), 1, 6.

[58] Kamrul Faisal, "Certain Legal Aspects of Children's Right to Protect Personal Data in the Context of AI under the European Union Data Protection Laws," in Vapaita sanoja: Viestintäoikeuden vuosikirja 2022 (Forum Iuris 2023), ed. Päivi Korpisaari, <https://www.edilex.fi/viestintaoikeuden-vuosikirja/1000870008.pdf>.

the ways in which children merit special protection,[59] specific transparency requirements for children,[60] or the fact that controller(s) must obtain consent from parental authorities before processing children's data.[61] The author does not discuss whether the phenomenon qualifies children for consideration as a separate category of data subjects. If so, then in addition to average and vulnerable data subjects, we may have another type of data subject under the GDPR, which may lead to the highlighting of distinct child-specific and vulnerable-specific settings.

Second, though it is clear that addressing a significant power-imbalance relationship helps identify vulnerable data subjects based on different layers, the book does not clarify the types of mechanisms that controllers might deploy or activate in vulnerability-specific data processing settings or systems when a significant power-imbalance relationship reaches a threshold of intolerability. It is necessary to identify such a threshold in a commonly understandable manner in order to successfully navigate the challenges that safeguarding mechanisms may require from the controllers precisely because different vulnerable individuals usually use the same services that are developed for average data subjects.[62] If this emerging legal principle requires that the systems change depending on the data subjects, then most likely we must understand the severity of the effect in a manner that helps controllers and other enforcers in a legally relevant way. Though we know that the processing of vulnerable people's data may create greater risks, we lack the knowledge of when such an instance occurs.

Third, while defining the vulnerability approach as a heuristic tool for interpreting the system of principles, rights, and impact assessments (that may force controllers to consider vulnerability), the author then proceeds to consider only a few specific ethical and legal standards. While a broader discussion may be beyond the scope of the study, it should be noted that not adequately examining ethical shortcomings may harm vulnerable data subjects. For example, the act of protecting vulnerable data subjects is associated with the principles of human dignity and human rights since vulnerable data subjects are more susceptible to misinformation and discrimination based on such factors as age, disability, health status, racial or ethnic background.[63]

[59] Recital 38, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR).

[60] REGULATION (EU) 2016/679, Article 12(1).

[61] REGULATION (EU) 2016/679, Article 8.

[62] Valerie Verdoodt, Yueming Zhang, and Eva Lievens, "Safeguarding the Child's Right to Privacy and Data Protection in the European Union and China: A Tale of State Duties and Business Responsibilities," International Journal of Human Rights 1 (2023): 1, <https://doi.org/10.1080/13642987.2023.2233917>.

[63] Malgieri and Niklas, "Vulnerable Data Subjects"; Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

In addition, protecting vulnerability helps preserve informational self-determination or human autonomy,[64] as well as trust between individuals, organizations, and society as a whole. Moreover, European laws protect vulnerable humans through certain *lex specialis*, which outline the dos and don'ts concerning certain vulnerable groups, like children,[65] the elderly,[66] persons with disabilities,[67] people who may be mistreated, victims of human trafficking,[68] asylum seekers,[69] victims of crime,[70] or clinical trial subjects.[71]

Lastly, the author only briefly touches upon the GDPR's rules concerning other high-risk specific requirements that the law vests in controllers, for example consulting the supervisory authority before processing,[72] informing the data protection authority and data subjects about any possible data breach,[73] or maintaining records of processing activities that may cause risk to data subject's rights and freedoms,[74] all of which might cause controllers to stumble into regulatory pitfalls. It is one of main responsibilities of controllers to protect vulnerable data subjects from all such hazards both by design

[64] Zohar Efroni et al., "Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing," European Data Protection Law Review 5 (2019): 352, 366.

[65] United Nations Committee on the Rights of the Child, "General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment," vol CRC/C/GC/2 (2021), <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjH1P_fzPODAxUZQVUIHfHkC68QFnoECBEQAQ&url=https%3A%2F%2Fdocstore.ohchr.org%2FSelfServices%2FFilesHandler.ashx%3Fenc%3D6QkG1d%252FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%252F5F0>.

[66] Convention on the Rights of Persons with Disabilities and Optional Protocol 2007, 1.

[67] Convention on the Rights of Persons with Disabilities.

[68] DIRECTIVE 2011/36/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims 2011, 1.

[69] DIRECTIVE 2013/32/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 on common procedures for granting and withdrawing international protection (recast) 2013 60; DIRECTIVE 2013/33/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 June 2013 laying down standards for the reception of applicants for international protection (recast) 2013, 96.

[70] DIRECTIVE 2012/29/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA 2012, 57.

[71] REGULATION (EU) No 536/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC 2014, 1.

[72] Article 36, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR).

[73] REGULATION (EU) 2016/679, Articles 33–34.

[74] REGULATION (EU) 2016/679, Article 30(5).

and default.[75] For example, social media providers may by default limit the visibility of certain posts containing sensitive data shared by vulnerable users.

## 3 Conclusion

Overall, the book offers a comprehensive exploration of vulnerability in the context of the GDPR, providing insights into how to conceptualize and identify it and the corresponding legal protection mechanisms. In conclusion, I highly recommend that legal scholars, practitioners, and students read the book in depth.

*Kamrul Faisal*
Doctoral Researcher, Faculty of Law, University of Helsinki.

The Generation AI project of the University of Helsinki (grant number 01331393) and the Eino Jutikkala fund of the Finnish Academy of Science and Letters (grant number 0222799-7) have provided financing for this work. Thanks are given to Laura Drechsler, assistant professor, and Elora Fernandes, postdoctoral researcher, both associated with the Centre for IT and IP Law (CiTiP), KU Leuven for their insightful feedback, which enriched the quality of this review. The author further thanks the reviewer(s) and the in-house language revision services.

[75] REGULATION (EU) 2016/679, Article 25.