Vulnerability in the Digital Age

Oreste Pollicino

Vulnerability in the digital age is primarily connected to the evolving digitisation of societies. Despite the benefits brought by technologies, particularly artificial intelligence, however, this new technological eco-system has also amplified the questions for fundamental rights and freedoms, inevitably touching on the issues of vulnerability. It is interesting how this concept has increasingly evolved not only within the scope of constitutional law and digital constitutionalism, but particularly within the framework of European law, where this concept has emerged as a compelling area to reassess the existing legal protections and challenges faced by individuals and entities interacting with digital systems. Therefore, this book, *The New Shapes of Digital Vulnerability in European Private Law*, edited by Crea and De Franceschi, provides a timely analysis of the multifaceted nature of digital vulnerability, its implications, and the evolving responses of European legal frameworks.

At the heart of digital vulnerability is the recognition that technological developments, from algorithmic decision-making to the pervasive use of artificial intelligence, have shifted traditional power dynamics. These shifts create asymmetries between the providers and users of digital services, raising questions about fairness, transparency, and accountability. The increasing reliance on automated systems, smart contracts, and personalised services means that individuals in their position of consumers, workers, or citizens, are exposed to risks that often exceed their ability to understand or control them.

In the chapter by Goanta, De Gregorio, and Spanakis, *Consumer Protection and Digital Vulnerability: Common and Diverging Paths*, the authors address how the traditional concept of the "average consumer" is no longer adequate in the face of digital markets. They argue that the stereotyped consumer personas, as reflected in the Unfair Commercial Practices Directive, fail to account for the structural asymmetries exacerbated by mass consumer surveillance and harmful profiling. Their contribution not only explores the theoretical implications of digital vulnerability but also critical-

ly reflects on practical case studies, calling for a system-level rethinking of European consumer protection law to address these complex issues.

Rodriguez de las Heras Ballell, in *Digital Vulnerability and the Formulation of Harmonised Rules for Algorithmic Contracts: A Two-Sided Interplay*, delves into the specific vulnerabilities introduced by algorithmic contracting. The author coins the term "algorithmic vulnerability" to describe how automation processes, while offering potential benefits such as efficiency and personalisation, also intensify existing vulnerabilities, particularly for consumers. This chapter highlights the duality of automation's impact, exacerbating vulnerabilities on one hand, while potentially offering mechanisms to address them on the other, also calling for harmonised rules to navigate this complex legal terrain.

The contribution by Arian, *Vulnerability in the Age of Metaverse and Protection of the Rights of Users Under EU Law*, outlines some of the emerging issues relating to interaction in the metaverse, the challenges it presents to users, and explores the legal and regulatory landscape of marketing in this digital environment, in particular analysing the rights of "vulnerable consumers" such as children and, more in general, assessing whether the metaverse dimension may exacerbate the vulnerabilities of vulnerable users by subliminally influencing their decisions in ways that may not serve their best interests.

In a related exploration of algorithmic automation, Golub's chapter, *Digital Vulnerability of Consumers in the World of Smart Contracts – Is European Private International Law "Digitalised" Enough?*, examines how smart contracts pose new legal challenges. The author questions whether European private international law is adequately equipped to handle these challenges and explores the need for adaptations in conflict-of-law protection to ensure that consumers, as the weaker party, are not unduly disadvantaged in these digital transactions.

The cross-border nature of digital interactions adds further complexity to the issue of vulnerability, as explored in the chapter by Goh Escolar, *Addressing Digital Vulnerability Through Private International Law*. This contribution addresses the uncertainties and gaps in jurisdictional and legal frameworks that arise from digitalisation. By discussing practical cases such as distributed storage mechanisms, digital currencies, and AI-driven contracting, the chapter illustrates how private international law must evolve to address the unique vulnerabilities inherent in a highly digitised global economy.

Tereszkiewicz, Południak-Gierz, and Walczak, in their chapter *The Digital Vulnerability of Insurance Consumers and Personalised Pricing of Insurance*, address the intersection of digital vulnerability, data protection, and personalised pricing in the insurance industry. Their analysis highlights how personalised pricing, when not properly regulated, can deepen consumer vulnerabilities and potentially violate GDPR provisions. They also examine whether such practices can be covered by the Unfair Commercial Practices Directive, pointing to the need for a more robust integration of data protection within consumer law.

Also, children and other vulnerable groups are particularly exposed to digital risks, as discussed in the chapter by Pera and Rigazio, *Let the Children Play. Smart Toys and Child Vulnerability*. Their examination of the digital vulnerability of children through the lens of smart toys underscores the need for specific legal protections tailored to the unique risks that digital environments pose to minors.

The medical field also faces its own set of digital challenges, as Amram explores in *Standards to Face Children and Patients Digital Vulnerabilities*. This chapter highlights the importance of establishing standards and methodologies that address the vulnerabilities of children and patients within digital care environments. It further discusses how digitalisation in healthcare necessitates new balances between care obligations and the protections afforded by the legal framework.

Workplace vulnerability is another pressing issue, as Wildhaber and Ebert discuss in *From Digital Vulnerability to Data Anxiety: The Situation of Employees in Digitally Permeated Workplaces*. Their empirical study on the impact of digital technologies on employees across various industries in Switzerland reveals how algorithmic management tools exacerbate feelings of vulnerability among workers. Their chapter suggests potential reforms, including strengthening collective representation and ensuring duty of care towards employee well-being.

The digitalisation of industries extends even to agriculture, as explored by Stiefel and Sandoz in *Design for Agency vs. Vulnerability by Design – The case of Swiss Agriculture*. Their contribution on the Swiss agricultural sector illustrates how competing digital platforms can create vulnerabilities for farmers and organisations alike, especially in terms of data management, centralisation, and trust.

In the concluding chapter, *Digital Vulnerability in European Private Law*, Schulze synthesises the various perspectives explored throughout the book and frames digital vulnerability as a cross-cutting issue for European pri-

vate law. He also underlines the role of the Digital Services Act which provides instruments to address some of the unsolved questions related to vulnerability in the digital age.

This edited collection provides indeed a comprehensive overview of the new shapes of digital vulnerability in European private law, also touching on critical questions for constitutional law. It offers critical insights into the challenges posed by digitalisation and proposes pathways for reform.