Digital Vulnerability for All

Marta Infantino and Camilla Crea

Abstract What if we took seriously the idea recently put forward by many institutions and scholars that, in online interactions, all human beings are vulnerable or made more vulnerable than ordinary? What if our regulatory infrastructures acknowledged that the vast majority of us, even in the hyperconnected societies of the Global North, have little understanding of the digital infrastructure on which we depend? This chapter aims to explore these questions and propose a new interpretive framework, using European private law as a testing ground at the crossroads of national and European Union rules. In particular, it investigates whether assuming that we are all vulnerable might reduce the protection for those who belong to protected categories and are at heightened risk of cumulative and intersectional discrimination. It tests whether embracing digital vulnerability as a universal condition would lead to an unacceptable level of personalization of the law and burden corporations and individuals with excessive vulnerability-related duties. The chapter also verifies whether and how vulnerability-related duties might be enforceable in the borderless digital environment. All of the above will hopefully help challenge current interpretive views that deny any relevance to online defenselessness.

Keywords Universal digital vulnerability · European private law · Digital fairness · Intersectionality · Platform liability · Peer-to-peer abuse

Camilla Crea is the author of Sections 2–4; Marta Infantino is the author of Sections 5–7. Sections 1 and 8 were coauthored.

M. Infantino (✉)
Department of Political Science, University of Trieste, Trieste, Italy
e-mail: minfantino@units.it

C. Crea
Department of Law, Economics, Management and Quantitative Methods, University of Sannio, Benevento, Italy
e-mail: camicrea@unisannio.it

C. Crea and M. Infantino (eds.), *Remedies to Digital Vulnerability in European Private Law*, https://doi.org/10.1007/978-3-032-19720-7_18

1 Introduction

In recent decades, the concept of vulnerability has gained prominence in many post-industrial societies, reflecting the increasing fragility of human beings, economies, infrastructures, and ecosystems in the contemporary world. The notion of 'vulnerable subject', in particular, has become a powerful and dynamic concept that explains how all individuals, including those who do not belong to traditionally protected categories, are universally vulnerable due to both their physical bodies and their inevitable dependence on social relationships and institutions.[1] While there are vulnerable subjects who are not human beings, such as minority groups and small enterprises, the following discussion will focus on individuals only.[2]

In the field of law, the concept of vulnerability has rapidly entered the lexicon and debates around consumer protection, both at the international level and in specific regions, such as Europe and Latin America.[3] In Latin America, the Mercosur Common Market Group imposed in 2019 the obligation on its member states to recognize the structural vulnerability of all consumers in offline and online markets.[4] In 2021 the same Group further required Mercosur states to adopt a wide range of measures (from information to protection against misleading and abusive offers, protection of data and privacy, and dispute resolution mechanisms) in order to protect 'hyper-vulnerable consumers', defined as individuals with aggravated vulnerability who are disadvantaged due to their age, physical or mental condition, social, economic, ethnic and/or cultural circumstances.[5] The notion of vulnerability had already entered the domain of European private law some years earlier, through specific interventions in consumer protection. At the beginning of the century, the first pieces of European Union legislation using the category were enacted,[6] and legislative references have multiplied since the 2010s, when it became clear that the digital transformation of the economy and society was creating new risks for

[1] Fineman (2008).

[2] Macioce (2022).

[3] See Infantino (2025).

[4] Mercosur (2019).

[5] Mercosur (2021). On this framework, see Martínez Alles (2025).

[6] See Directive 2001/95/EC on general product safety, recital 8, and Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market (UCPD), recital 18 and article 5(3). The EU Charter of Fundamental Rights does not refer to vulnerability, but mentions in articles 23–26 specific categories of people—women, children, the elderly and disabled persons—as deserving peculiar protection.

consumers.[7] In contemporary European legal terminology, vulnerability is associated with the structural asymmetry of consumers in the digital marketplace.[8] This digital version of real-world vulnerability is commonly defined as the "universal state of defencelessness and susceptibility to (the exploitation of) power imbalances that are the result of increasing automation of commerce, datafied consumer-seller relations and the very architecture of digital marketplaces".[9] It should be noted that the use of 'digital' in this context should be understood broadly, in a manner similar to Floridi's notion of 'onlife'.[10] For example, people's vulnerabilities can be abused or exacerbated by algorithmic devices, even when they are not using them: imagine someone without a social media account being bullied online, or a patient receiving a false cancer diagnosis from a doctor who follows the recommendations of an AI-driven program.

In the following pages, we will examine the implications and limitations of the concept of digital vulnerability in European private law. We will not discuss EU law per se, but rather European private law, by which we mean the combination of national and supranational private legal rules and principles applying in Europe. We are aware that this is a simplification of a very complex picture, and that further comparative studies are needed to test the validity of what is proposed here.[11] Yet, for the purpose of this chapter, whose main contribution lies in the proposal of a new interpretive framework, we believe it is legitimate to situate it within the realm of European private law. Since our perspective is centered on private law, we will not focus on perspectives other than those of private law, even though we acknowledge that other legal approaches—such as those offered by digital constitutionalism and public regulation of digital markets—do exist and operate in parallel with private law remedies.

More specifically, the chapter aims to explore the private law implications of people's "universal state of defencelessness" in the digital world. To this end, we will begin by challenging the notion that digital vulnerability arises solely in transactional situations, as current EU law assumes (Sect. 2). We will then argue that digital vulnerability should be understood as a broad concept, capable of encompassing both the universal status of people online and the particular status of situated subjects, along with all the layers of vulnerability they may possess (Sect. 3). After examining a real case to illustrate our point (Sect. 4) and addressing the most common objections

[7] See, for instance, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), recital 75; Regulation (EU) 2022/2065 on a Single Market for Digital Services (DSA), recitals 62, 69, 94–95, 104; Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AIA), recitals 29, 48, 58, 60, 67, 93, 132, 141, 165, and article 5(1), letter (b), 7(2), letter (h), 9(9), 60(4), letter (g), 79(2), 95(2), letter (e).

[8] Crea and De Franceschi (2024).

[9] Floridi (2015).

[10] BEUC (2021, 94).

[11] So far, the only European country that has enacted specific rules on vulnerability is Spain: see Ley 4/2022, de 25 de febrero, de protección de los consumidores y usuarios frente a situaciones de vulnerabilidad social y económica.

to the possibility of adopting a broad notion of digital vulnerability (Sect. 5), we will demonstrate the potential consequences of taking vulnerability seriously. We will emphasize that addressing digital vulnerability implies the emergence of new obligations for digital actors (Sect. 6). We will then test the practical implications of our proposal and verify whether such a world of new rights and duties might actually work in practice (Sect. 7), distinguishing the consequences for companies, including digital service providers (Sect. 7.1), and for individuals (Sect. 7.2). We will conclude with some final thoughts on the prospects for digital vulnerability (Sect. 8).

2 The Digitally Vulnerable Subject Beyond the Consumer/User Paradigm

There is no doubt that the complex genealogy of the notion of digital vulnerability, along with its multidisciplinary and multidimensional nature, contributes to critically deconstructing, fragmenting, and reshaping new images of the consumer. The growing EU consumer legislation that explicitly focuses on consumers' digital vulnerability,[12] together with recent rulings by the Court of Justice of the EU (CJEU),[13] demonstrate the growing importance of this idea in today's economy. There is indeed much empirical evidence that the ever-increasing power of technology to collect data and channel customer behavior has favored corporate strategies, such as data harvesting and data mining, dark patterns, targeted advertising, price optimization, and algorithmic personalization, that pose high risks of harm, along with new forms of consumer commodification in the context of digital consumption.[14] For this reason, many scholars have argued that the EU should ban or automatically consider these practices unfair,[15] or establish a presumption that all consumers are vulnerable in their relationships with traders in the digital realm.[16] From such a perspective, the idea of digital vulnerability has the potential to challenge some of the conventional paradigms arising from the EU neoliberal approach to consumer protection.[17]

This vision, however, is not fully in line with the European Commission's approach and agenda. The very recent Fitness Check on EC consumer law retains many of the above premises, going as far as to state that "[t]he provisions on the 'average consumer' and the 'vulnerable consumer' may need to be further clarified or amended to ensure their effectiveness in the digital context".[18] Yet, in the study supporting

[12] See above, notes 7–8.

[13] Court of Justice of the European Union (CJEU), case C 646/22, *Compass Banca*, ECLI:EU:C:2024:957, no. 59.

[14] European Commission (2024a, 177–197, 209–216), European Commission (2016).

[15] Micklitz et al. (2024); BEUC (2021, 5).

[16] Riefa (2022, 611).

[17] Krämer (2021, 13–19).

[18] See European Commission (2024b, 48).

the Fitness Check, the European Commission framed digital vulnerability not as negative per se, but rather inasmuch as it raises "concerns in terms of collective welfare due to detrimental effects on competition, price transparency and trust in the market".[19] In other words, according to the European Commission, consumers' digital vulnerability is bad because it damages the market. This understanding clearly limits the revolutionary potential of the notion of digital vulnerability, restricting it to business-to-consumer (B2C) relationships and subordinating it to the "original ambivalence of the European integration project"[20] and the underlying "spell"[21] of the internal market. Under this spell, dominant EU narratives and legal policies continue to assume that individuals ought to be (digital) market actors. From this perspective, consumers are rights holders deserving protection only insofar as they engage in acts of consumption.[22]

To be fair, some recent EU legislation has adopted a different vision of (digital) vulnerability, extending the paradigm of the vulnerable consumer to include citizens who are vulnerable to organs of public administration and infrastructures. For example, in addition to the usual references to vulnerable users of online corporate services, the recent Artificial Intelligence Act (AIA) mentions several cases in which people are, or are made, vulnerable by their interactions with public authorities—what we might call consumer-to-government (C2G) relationships.[23] Underlying this broader approach, however, is still a market-driven mentality that sees people's vulnerability in accessing and using public services as a bad thing, as it undermines the efficiency of the government, and people's trust in it. This expanded view of digital vulnerability, encompassing both B2C and G2C relationships, should therefore be seen as the result of the inclusion of government infrastructure in the digitization agenda, rather than as a change to the traditional, market-oriented view of vulnerability.

We claim that, by relying on these assumptions, the European debate on consumer digital vulnerability misses a substantial part of the picture. The problem is not just that the definition of vulnerable consumers under EU law remains too rigid and narrow, covering only a small number of stereotypical grounds for vulnerability and failing to address the wider power imbalances affecting the digital market.[24] The problem lies in the market-driven perspective, which fails to highlight all the injustices that occur beyond the realm of structurally unbalanced relationships between businesses and governments, on the one hand, and consumers of private and public services, on the other hand. While the lion's share of toxic interactions in the digital sphere is undoubtedly managed by service providers that exploit people's vulnerability, this focus on consumers obscures all forms of (exploitation of) vulnerability that occur in digital relationships with no, or an unclear, commercial character.

---

[19] European Commission (2024a, 44). For some observations in line with the text, see Gellert (2024).

[20] Bartl (2015, 573).

[21] Caruso (2012).

[22] Schulze and Staudenmayer (2024).

[23] Recitals 58, 60 and articles 7(2), letter (h) AIA.

[24] See the authors mentioned above, notes 15–16, as well as European Commission (2024b).

Suffice it to recall the various scams, cyber-bullying, revenge porn, social media shitstorms, disinformation campaigns, fake news spreading, and dangerous challenges on social networks. In all these situations, the binary opposition between 'vulnerable consumer' and 'trader' does not adequately address the complexity of human interactions in digital ecosystems.

The concept of consumer vulnerability currently embraced by the EU institutions does not cover all the various possible sources and layers of asymmetry, injustice, and inequality that can affect human beings far beyond the traditional categories of vulnerable subjects. Despite the apparent legal consensus on the challenges that 'digitization' poses to human rights,[25] the EU's current recipe still relies on a formal, market-based dichotomy that fails to capture the many fragmentations of subjectivity and does not take into account the inherent intersectionality of digital vulnerability.[26] As such, the current approach remains unable to effectively achieve equality and social justice on the one hand, and to overcome the abuse of consumerism and the dominant logic of capital on the other hand.[27]

How can this approach be challenged and its limitations overcome? We propose considering vulnerability as a universal and particular condition of all connected individuals, regardless of whom they are facing. We will now attempt to clarify our meaning.

3 Digital Vulnerability as Universal and Particular

When we suggest that vulnerability should be seen as a universal and particular condition of all connected individuals, we mean that it is high time to accept that the fictional narrative about the average consumer being "reasonably well-informed and reasonably observant and circumspect", first developed by the CJEU[28] and now enshrined in the UCPD,[29] may not be a generally good fit, but it certainly does *not* fit the digital economy. The truth is that we, or at least the overwhelming majority of us, are ignorant of the digital infrastructure, its costs, its opportunities and its alternatives, and we passively accept every opportunity that comes our way.[30] We remain ignorant and passive, regardless of whether we are given access to information and the opportunity to read the detailed terms and conditions of the services we receive. The online world is entirely made up of the architectural and contractual

[25] BEUC (2021).

[26] In relation to privacy law, see Malgieri (2023).

[27] Pistor (2019).

[28] CJEU, case C-210/96, *Gut Springenheide and Tusky v Oberkreisdirektor des Kreises Steinfurt*, ECLI:EU:C:1998:369; CJEU, case C-220/98, *Estée Lauder Cosmetics GmbH & Co. OHG v Lancaster Group GmbH*, ECLI:EU:C:2000:8. More recently, CJEU, case C 646/22, *Compass Banca*, ECLI:EU:C:2024:957.

[29] Recital 18 of the UCPD.

[30] See the empirical studies mentioned above note 19.

affordances set up by corporations, whose private governance of the online world is sometimes constrained by national laws.[31] To accept that our exposure to highly asymmetrical relationships makes us all vulnerable is to recognize that online vulnerability is universal, and can be presumed to be so. This, of course, does not preclude the possibility that categories other than people may be vulnerable, nor that there may be a few individuals (e.g., a skilled computer scientist) who may not be vulnerable at all.[32]

The assumption that digital vulnerability is universal, moreover, does not exclude the possibility that vulnerability can also be specific. Digital vulnerability often does not exist in isolation, as it may combine with other subjective and situational strengths and weaknesses of the digitally vulnerable person. In other words, the idea that everyone is vulnerable online does not preclude also recognizing that some are more vulnerable than others—what we may call, following the approach in the Mercosur—'hyper-vulnerable' subjects.[33] In particular, the factors stereotypically associated with vulnerability in the real world also apply in the online one. In this regard, the European Commission's recent Fitness Check explicitly mentions age and disability (and occasionally adds having a migrant background),[34] but broader lists can easily be imagined. Just think of all the factors mentioned in the EU Charter of Fundamental Rights and the European Convention on Human Rights and Fundamental Freedoms (ECHR) as potential bases for discrimination,[35] or of the special features listed in article 9 GDPR as giving rise to a significant risk to the fundamental rights and freedoms of the person concerned.[36] When digital vulnerability coexists with an additional factor/driver of vulnerability, it creates an intersectional vulnerability, meaning a combined form of vulnerability, the consequences of which are often worse than the mere sum of each factor/driver of vulnerability.[37]

This universal and particular vulnerability online is invariably exploited in B2C (and occasionally in C2G) relationships.[38] Our point, however, is that digital vulnerability may be exploited even outside of a commercial (or of a state-citizen) relationship. Digital vulnerability can also be exploited by others, although they often do so through the mediation of search engines, online platforms, and social networks. In other words, the digital infrastructure managed by corporate private powers enables both the abuse of these powers and of what we may call peer-to-peer abuse. This brings us to a paradox inextricably associated with the human

[31] On BigTech acting as virtual governments, see, e.g., Lee (2022); Lessig (2006).

[32] Assuming that everyone is vulnerable does not preclude proving that someone is not. Another practical issue arising out from the presumption concerns the difficulty of distinguishing individuals from empty avatars, bots, and AI-driven machines. On this issue, see also below, Sect. 7.2.

[33] Malgieri and Niklas (2020); on the Mercosur approach, see above, Sect. 1.

[34] See European Commission (2024b, 39–40, 43, 167).

[35] See article 21 of the EU Charter and article 14 of the ECHR.

[36] GDPR, article 9.

[37] The concept of intersectionality travelled from US to Europe: Crenshaw (1989); Hesselink and Soei Len (2025).

[38] European Commission (2024b).

condition in the digital sphere, extending beyond the structural asymmetrical field of commercial transactions, i.e., the opposition between dependence and independence, between vulnerability and autonomy. In the digital context that exists beyond commercial relationships, individuals enjoy both a reduced level of autonomy ('hypo-autonomy', compared with the hyper-autonomy of technological companies), making all of them structurally vulnerable, and broad agency in their peer-to-peer relationships with other individuals ('hyper-autonomy' in consumer-to-consumer (C2C) relationships).[39]

On the one hand, people's hypo-autonomy stems from their subjection to the online architecture/design, business strategy and private governing power of digital service providers. Under the current EU framework, including both traditional consumer law measures[40] and the newest interventions in the digital environment,[41] people matter and are protected because they are (occasionally vulnerable while) acting within the universe of consumption or post-consumption.[42]

On the other hand, human beings enjoy a broad freedom/power of action that allows them to misuse and weaponize their access to digital tools—more or less consciously—against their digitally vulnerable peers. This broad freedom is often strengthened by the anonymity provided by the use of online usernames and avatars concealing individual identity and by the crowd of other abusers. While it cannot be stressed enough that this hyper-autonomy only exists to the extent that companies allow it to, the end result is that any online user has the ability to harm others with little effort and unparalleled efficiency.

This is the core and conundrum of digital vulnerability of persons: everyone is, at the same time, both digitally vulnerable (hypo-autonomous) *and* digitally autonomous when interacting with other individuals since anyone can cause harm to their peers (and, in turn, be harmed by them). This form of *coincidentia oppositorum*[43] arising from the complex notion of digital vulnerability generates new and complex power dynamics that we can explain in terms of the *interdependence of digital vulnerability*. The *interdependence* of digital vulnerability is intended to signify the importance of human beings beyond their consumer status, the intersectional character of digital vulnerability, and the circumstance that, in the digital world, all human beings are potentially both agents and victims of abuse. A notion of

[39] Domurath (2024).

[40] The reference goes to the Council Directive 93/13/EEC on unfair terms in consumer contracts (UCTD) (prohibiting unfair clauses in B2C contracts), the UCPD (prohibiting aggressive and misleading commercial practices), and the Directive 2011/83/EU on consumer rights (CRD) (providing consumers in off-premise contracts with informational rights and the right of withdrawal).

[41] Think of the Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (DMA) (prohibiting certain clauses and practices in commercial online relations), the DSA (establishing some obligations on online platforms and search engines), the Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act) (providing users with the right to access and share the data produced by connected products), the AIA (prohibiting some AI-driven practices and regulating high-risk uses of AI, as well as generative AI).

[42] Grochowski (2024).

[43] Teubner (2006).

digital fairness that extends beyond the traditional consumer-victim paradigm must embrace the *interdependence of digital vulnerability*.

4 Imane Khelif and Digital (Un)Fairness

Let us take a possibly extreme case of interpersonal injustice to illustrate the above-mentioned gaps in European legal discourse, revealing its blindness to certain issues and the urgency of finding solutions.

Imane Khelif's victory in a boxing match against Angela Carini at the 2024 Paris Olympics ignited a global debate fueled by accusations concerning Khelif's gender identity and fairness in sport. Despite complying with IOC regulations, Khelif became the victim of a wave of transphobic and sexist abuse online. Khelif was attacked for her appearance and perceived sexual characteristics, but it is hard to ignore the fact that she was a Muslim woman of color representing a non-Western country in a typically male sport like boxing. The controversy was amplified by the intervention of public figures such as Elon Musk and J.K. Rowling (whose comments on X received more than 11.8 million views), thus highlighting wider issues of social injustice and discrimination. Notwithstanding this, Khelif won the gold medal. In response to the online shitstorm that hit her with millions of insults and threats on a variety of social networks, some days later she filed a legal complaint against social media platforms, prompting an official investigation into cyber harassment in France.[44]

Khelif's case is exceptional in that it involves a top Olympic athlete who, by definition, is not the average person on the Clapham bus. However, it is also very typical of the kind of online harassment that can affect people and have a lasting impact in the real world. The case is instructive for us because it clearly shows that everyone, including the top-performing and physically strong, is vulnerable online. It also shows the intersectionality of vulnerability at play. Khelif's digital exposure was exacerbated and amplified by her combination of many grounds that potentially increase the risk of discrimination, such as her non-conforming femininity and alleged transsexuality, her Muslim faith, and her non-Western background. Most importantly, the case demonstrates how easily people can be abused through the intermediary of digital services provided by private companies. The online harassment was made possible by the availability of social networks whose content moderation policies are based on the principle of protecting freedom of speech, and whose business model favors the fastest and widest distribution of viral content, as divisive issues typically are. Yet the online harassment was actually carried out by people (arguably with the help of some bots), who wrote, shared, liked, posted and reposted comments that were then matched by machines and allowed to circulate worldwide. This shows the point we were trying to make earlier: in the digital world, we are all potentially both victims and perpetrators of abuse.

[44] For the facts of this case, see https://www.washingtonpost.com/sports/olympics/2024/08/15/imane-khelif-cyberbullying-complaint/.

The protection of digital vulnerability beyond the consumer paradigm must somehow embrace this paradox and accept the *interdependency of digital vulnerability*. Accepting this paradigm would mean recognizing the duty of care owed by anyone who abuses or exploits digital vulnerability, regardless of their status and position. We will explore this in more detail in Sect. 6 and then provide suggestions on how it might be implemented in practice. Before we get there, we need to spend some time defending our proposal against the objections that are commonly raised against the idea of adopting a(n either broad or narrow) notion of digital vulnerability.

5 Countering Common Objections to Vulnerability

In the legal domain, vulnerability talks tend to trigger a number of objections that we would like to address before going any further, for we imagine that they might be also raised against the proposal we are making here. In essence, our proposal is based on the idea that everyone, or at least the vast majority of people, is vulnerable in their interactions with digital devices, or is made vulnerable by them. This is so true that we could (or rather should) assume that everyone is vulnerable online—in other words, that the average online state is one of vulnerability. Non-vulnerability is the exception. Such a conclusion does not exclude the possibility that many people, particularly those belonging to protected categories at heightened risk of discrimination, may be made extremely vulnerable by the intersection of digital vulnerability with various factors/drivers of vulnerability. The likelihood of this happening suggests that whenever a person with multiple possible drivers of vulnerability complains of abuse, it can be assumed that these factors/drivers have been triggered; in other words, it can be presumed that these persons are hyper-vulnerable. Finally, we argue that since digital vulnerability is invariably exploited by companies and in particular digital service providers, but also occasionally by other individuals, these subjects should be considered to have a duty not to abuse the vulnerability of others. Is there any reason not to want such a broad notion of vulnerability to be recognized? In the following lines, we will consider some of the common objections that are typically raised against the idea of vulnerability, and try to see if any of them pose an insurmountable obstacle.

1. Vulnerability is a category that is too subjective and variable to be taken seriously into account by the law. Adopting the lens of vulnerability would break the equality of the law and undermine legal certainty, filling the world with granular rights and duties whose contents are hard to predict.

The problem of the extent to which rules should be abstractly tailored to an ideally average subject or should rather consider (at least some of) the characteristics of the people involved is a longstanding problem that contemporary legal systems in the

West have solved by favoring formal equality.[45] But the emergence of new technologies that are increasingly able to identify people's characteristics has reignited the debate about the extent to which rules can and should be personalized.[46] Leaving aside any broader consideration on the many departures that legal systems accept from the idea of formal equality (including anti-discrimination rules), the point is that we are proposing to consider digital vulnerability as a universal condition. Everyone would be treated equally in this scenario, without the need to check whether someone is actually vulnerable or not. Formal equality and legal certainty would be guaranteed. The presumption could, of course, be rebutted if, exceptionally, there were no vulnerability.

2. Protecting certain vulnerable categories undermines equality and privileges them over the ordinary rest, sometimes reversing the power imbalance against innocent 'average' people. There is already a rights fatigue in contemporary societies; protecting people's digital vulnerability would create another unnecessary privilege.[47]

It is true that automatically categorizing people with certain characteristics as vulnerable is a stereotypical classification that may not reflect reality and lead to overprotection. However, our proposal here is that everyone, including the ideal average person, is vulnerable or made vulnerable by interacting with digital devices. Moreover, because we live in unequal societies where many groups are at risk of mistreatment by a silent majority, we propose that additional factors of vulnerability should be presumed whenever the individual concerned falls into a protected category. It is not a privilege to be in this category. The presumption, like the average digital vulnerability presumption, would leave it open to individuals to demonstrate that they or their counterparts are below or above this average level of vulnerability.

3. If everyone is vulnerable, then no one is. Too high a standard of protection would dilute the meaning and rationale of vulnerability.[48]

This fear too is unfounded. On the one hand, the fact that everyone is vulnerable in the digital environment does not preclude the possibility that some people are more vulnerable than others (and that some people are not be vulnerable at all). Because digital vulnerability is often combined with other historically recognized factors or drivers of vulnerability, we propose that a presumption of intersectional vulnerability should automatically help people in protected groups. Like any presumption, it could be disproven. On the other hand, it is important to remember that we are suggesting that everyone is potentially both a victim and a perpetrator. The fact that everyone is vulnerable online is precisely the reason why everyone should be vigilant for other

[45] On the limitations arising out from this choice, Calabresi (1985, 22–25), Chamallas and Wriggins (2010, 89–117).

[46] For the terms of such a debate, Ben-Shahar and Porat (2021). For some critical remarks, see Endicott and Young (2022); Burk (2021).

[47] The argument is a recurring one in the field of human rights: Theilen (2021); Clément (2018).

[48] This argument is often intertwined with the one mentioned above, note 47.

potential vulnerabilities. In other words, a high standard of protection does not dilute the meaning of that protection; rather, it creates meaningful duties.

4. The idea that we are all vulnerable is paternalistic in that it assumes that we are all powerless, incapacitated victims and in need of protection.[49]

Legal systems, especially those in the civil law tradition, are well-acquainted with rules that create mechanisms of protection, limiting people's freedom to protect their dignity. To some extent, all consumer law can be seen as a paternalistic system of consumer protection. Respecting formal equality in an unequal world would only lead to more inequality.[50] In addition, we propose that digital vulnerability should be presumed, meaning that everyone should remain free to prove that they or their counterpart are not vulnerable, but rather fully informed, fully cognizant, fully aware. Finally, the fact that we are all vulnerable to abuse by others creates an obligation for everyone not to exploit the vulnerability of others. Recognizing the universality of vulnerability is not just a matter of protection; it is also a matter of recognizing the universality of a duty to protect.

5. Taking care of everyone's vulnerabilities imposes unbearable and near-impossible duties on companies, governments, and individuals acting in the digital world. They would be required to conduct countless checks and provide constant care to anticipate who might be or will become vulnerable due to interaction, and to somehow incorporate this prediction into their actions.

It is undeniable that to assume that everyone is vulnerable online implies the creation of additional duties for all actors in the digital world. This would be in line with developments in private law over the last two centuries in the West. Private law has consistently followed the rise of innovative technologies and the invention of new techniques for creating harms, with the establishment of duties for those who cause such harms.[51] Most importantly, private law obligations always exist in context, in the sense that they affect people differently according to their power, ability, expertise, knowledge and capacity to prevent harm. Clearly, those in a structurally unequal relationship with online users, such as search engines, online platforms, and social networks, who have the opportunity to know them, would have a greater duty to identify those who are most vulnerable and therefore in need of heightened protection.[52] The duty of others would largely depend on their ability to understand and care for the vulnerability of others, as well as other contextual factors such as their visibility and authority, the severity and seriousness of the attack, the number of people involved, and so on. We now need to look more closely at the implications of this new duty.

---

[49] The paternalistic objection is well-known in debates about vulnerability: Mackenzie (2013, 46–48), Kohnt (2014).

[50] This argument too is commonly raised against the idea of recognizing new human rights: Theilen (2021, 848).

[51] Bussani, Sebok, Infantino (2022, 213–247).

[52] For similar observations, see Malgieri (2023, 196–205).

6 Taking Digital Vulnerability Seriously

If our theoretical assumptions are correct, then the crucial question becomes: what can be done? What can private law do to effectively reshape digital vulnerability?

The starting point of our response is that there can be no right without a corresponding duty. The assumption that vulnerability is both a universal and a particular condition of all persons online necessarily requires imagining corresponding, relational duties for all actors in the digital domain, including corporations, public administrations and individuals. In continental European legal systems, the duties incumbent on public administrations are traditionally considered to belong to the realm of administrative law and public law in general.[53] As our focus is on private law, we will leave public administrations out of our analysis, and discuss the issue of duties toward companies and digital service providers on the one hand, and people on the other.

Companies offering goods and/or services online are already subject to many obligations vis-à-vis consumers, including those stemming from EU consumer law (the UCTD, the UCPD, and the CRD) and data protection law (mainly, but not exclusively, the GDPR). Adopting the view that everyone online is vulnerable and that traders should presume this vulnerability does not imply the emergence of new duties, but rather a different interpretation of existing ones. For example, the concepts of universal and particular vulnerability would significantly affect the interpretation of the transparency requirement in standard consumer contracts as laid down in article 5 UCTD, the paradigm of the average and vulnerable consumer under article 5 UCPD, the information obligations in distance contracts under articles 5–8 CRD, and the technical and organizational measures needed to address risks for personal data under article 24 GDPR, and so on and so forth.[54]

A different argument should be made for providers of digital intermediary service providers. While not all digital intermediaries are the same, it remains true that the largest among them, and in particular the largest search engines, online platforms, and social networks, are the primary source of people's digital vulnerability, insofar as they actively exploit the structural power asymmetry of their position and passively enable others to commit abuses. In relation to duties in the digital realm, there is little doubt in our view that the obligations of digital service providers should be extended beyond the current limits of the EU legal framework. The DSA has recently moved in this direction. On the one hand, the DSA confirmed the immunity of all digital service providers for content uploaded or posted by users,[55] as under the regime previously in force under Directive 2000/31/EC.[56] Under the DSA, digital service

[53] On the possible prospects of actions arising out from people's digital vulnerability brought against public bodies, see Infantino and Bussani (2025, 455–460), Infantino and Wang (2019, 351–352).

[54] For a similar proposal, see Riefa (2022).

[55] DSA, articles 4–6.

[56] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. This immunity was inspired by the enactment in the US

providers can be held liable only if they fail to remove defamatory posts and objectionable content promptly after being notified of their existence and ordered to do so[57]: this is the famous 'notice and take down' approach, different from the American rule, which enshrines the 'notice and stay down' approach.[58] On the other hand, the DSA establishes differentiated obligations for different types of digital service providers, requiring online platforms to design and operate their online interfaces in a way that does not deceive or manipulate users, and to provide users with information about the parameters of targeted advertising and recommendation systems.[59] The same Act adds that "[r]ecipients of the service shall have the right to seek, in accordance with Union and national law, compensation from providers of intermediary services, in respect of any damage or loss suffered due to an infringement by those providers of their obligations under this Regulation".[60] The DSA thus combines the old idea that the immunity of digital service providers is key to the development of digital infrastructures, online freedom of expression, and e-commerce without fear of liability,[61] with the awareness that such immunity cannot become a patent violation of the principle that 'with great power comes great responsibility'.[62]

The possibility of recognizing the existence of new duties upon digital service providers is therefore facilitated in Europe by at least three factors. First of all, in the vast majority of European jurisdictions, contracts require no consideration to be binding, and consequently, there is little doubt that digital service providers are bound by contracts with users.[63] While this means that digital service providers may rely on standard terms and conditions to govern their relationship with users, it also means that general rules of contract law—including those on invalid terms, unconscionability and in good faith—may apply.[64] Second, the DSA imposes some statutory obligations on digital service providers, including direct obligations (e.g., information duties) and indirect obligations (e.g., the removal of defamatory posts when ordered). If interpreted broadly, these rules provide a statutory basis for obligations. Third, even outside the scope of these statutory provisions, all European private law systems contain general rules on non-contractual obligations, such as torts and unjust enrichment, which, in certain circumstances, oblige companies not to cause, and not to allow third parties to cause, damage to users or be unjustly enriched at

in 1996 of Section 230 of the Communications Decency Act (CDA) to immunize providers of 'interactive computer services' from liability for content posted by third parties.

[57] DSA, articles 4–10 and 54.

[58] Bradford (2023, 42–50, 116–118).

[59] DSA, articles 25–27. Article 28 DSA provides additional obligations for the protection of minors.

[60] DSA, article 54.

[61] See especially Bradford (2023, 46–52).

[62] See especially Bradford (2023, 42–50), Keats Citron (2022, 82–104).

[63] This position is now claimed also with regard to common law countries: see Mills (2024); Balkin (2020).

[64] On the potential of such rules, see Smits (2014, 136–157).

their expense.[65] In Europe, therefore, there are already many bases for placing duties on digital service providers that coexist with their immunity for users' activities. Interpreting such duties in a way that includes the consideration of people's digital vulnerability would create an incentive for digital service providers to internalize the social costs of their economic activity. Rather than being revolutionary, this would confirm the role that private law has played in industrialized legal systems over the last two centuries, distributing the massive losses associated with emerging technologies and finding a sustainable compromise between economic activities and the safety of products in mass consumer societies.[66]

Strengthening the obligations and rules regarding the liability of digital service providers is however only part of the solution. If we embrace the idea that all human beings are digitally vulnerable and have the right not to be abused, we must also assume that all digitally vulnerable individuals owe a duty of care to their peers when interacting in the digital context. Such a duty of care implies the obligation to respect and protect others and their dignity from moral, economic, and social harm within the digital ecosystem. This would not actually be anything new, as many such obligations already exist. The non-discrimination obligation contained in the EU Charter and the ECHR is, according to the CJEU, a horizontal obligation binding on everyone.[67] All European countries, albeit with varying rules, strike a balance between the constitutionally protected right to expression and the duty not to engage in activities that lead to defamation.[68] More broadly, as already mentioned, the extra-contractual obligations not to harm one's fellow human beings and to return unlawfully obtained benefits obtained are recognized in all European countries, although in different shapes and sizes.[69] It goes without saying that this peer-to-peer liability should co-exist with (and neither excuse nor diminish) the liability of digital service providers that manage the digital infrastructure enabling peer-to-peer abuse. It is equally obvious that this peer-to-peer liability should be administered taking into account the varying abilities of people to understand and cope with the complexities of digital society, i.e., that the extent of users' duties should be proportional to their ability to foresee, control, and mitigate harm.[70]

Implementing digital solidarity and pursuing social justice and equality in European private law should require the protection of the (universal and particularistic)

---

[65] For a survey of such rules, see Bussani, Sebok, Infantino (2022); Infantino and Wang (2019, 346–353). This point is also acknowledged in American literature: see Kaplan and Gordon-Tapiero (2024).

[66] See the authors quoted above, note 51.

[67] According to the CJEU, the general principle of non-discrimination enshrined in Article 21 of the EU Charter has horizontal direct effects, meaning that it should be respected not only by MS but also by individuals: CJEU, case C-144/04, *Werner Mangold v Rüdiger Helm*, ECLI:EU:C:2005:709; CJEU, case C-414/16, *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V.*, ECLI:EU:C:2018:257. See Colombi Ciacchi (2019).

[68] Such rules are however very different from place to place: De Gregorio (2022, 157–215); Tsomidis (2022).

[69] On this point, see above, note 65.

[70] As is common in private law liability claims: Bussani, Sebok, Infantino (2022, 27–42).

digital vulnerability of all human beings, as well as the recognition of obligations and duties on both the corporate actors that govern and shape digital ecosystems and online architectures and all the members of society who use digital technologies. Embracing such a shift would require a change in the current interpretation of existing legal norms, but this better use of the various resources of private law would make it possible to strengthen the protection of individuals without resorting to regulatory oversight or new reforms. This imaginative reconstruction, which may be considered radical in the current legal and academic context, could have significant consequences, as further explored below. The next section attempts to demonstrate how this could happen in practice.

7 Going Practical

Presuming that everybody is vulnerable online would imply that anyone operating in the digital environment has a duty to take other people's vulnerability into account. As noted above, such a duty would bind both businesses and individuals, albeit with different degrees of intensity. The duty to take digital vulnerability seriously would inform businesses' responsibilities to consumers and data holders online. It would imply a duty on all digital service providers not to profit, or allow others to profit, from people's digital vulnerabilities. It would include a duty on users (proportionate to their position and ability) not to exploit other users' digital vulnerability. Going into the details of what these duties might imply in concrete situations is largely beyond the scope of this article. Rather, we wish to address a practical objection to all of the above that may cast a shadow on the feasibility of our proposal: even assuming that such duties exist, could their breach somehow be enforced?[71]

This practical question can be further subdivided into several more specific questions. What would the legal basis for a claim based on a failure to consider people's vulnerability be? Assuming that a basis for the claim could be found, where would the claim be heard? As we already noted, companies and individuals in the digital domain who exploit other people's vulnerabilities can be located anywhere in the world: the digital domain by definition is not bound by territorial boundaries. In the current absence of any supranational regulation of cyber-torts,[72] the virtual location of the accident and its transnational nature make it hard to understand which jurisdiction is appropriate to hear claims arising from a digital wrong. Under what conditions could a claim be brought in Europe? Would the law of a European country apply? Even if the answer to these questions is in the affirmative, another major problem would arise from the defenses available. Companies can invoke the disclaimers and

[71] On the difficulties related to cyber-harms, Infantino and Bussani (2024, 292–309); Infantino and Wang (2019).

[72] The only international treaty so far is the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law adopted at Vilnius on 5 September 2024. See https://rm.coe.int/1680afae3c.

user assumption of risks clauses contained in the contractual standard documents they ask users to agree to.[73] In addition, digital service providers can rely on the regulatory immunities provided by the DSA.[74] Individuals can shield themselves from liability by arguing that they were exercising their constitutionally protected freedom of expression; and, in all cases where several people were involved in the harmful activity, any one of them can claim that their involvement was minimal and therefore not the cause of all the harm.[75] Lastly, additional difficulties in claims involving individuals would arise from the fact that most people online act under pseudonyms or use digital agents (such as avatars), which further complicates the search for identification, and that the people involved in cyber-torts are typically not only numerous, but also scattered across different states.[76]

Let us see in detail whether and how these problems can be solved for corporate (Sect. 7.1) and peer-to-peer (Sect. 7.2) abuses.

7.1 Corporate Abuses

The recognition of digital vulnerability as a universal and particular condition for everyone online would shed new light on the many obligations that companies offering goods and/or services online have toward their counterparts under EU consumer and data protection and national contract law, as well as on the specific obligations that arise for digital service providers under the DSA. Moreover, independently of these rules, each European legal system has general rules on non-contractual obligations, and in particular on tort and unjust enrichment, which oblige those who have unlawfully caused damage to another or who have unjustly enriched themselves at the expense of another to pay compensation or return what has been unlawfully obtained. It is true that in most cases the standard terms and conditions and other contractual documents that companies require online users to accept, contain clauses that limit the companies' liability for breach of contract, statutory breach, tort, and unjust enrichment and provide for choice of law and dispute resolution clauses that point to laws and jurisdictions that are different from those of the users.[77] This may not constitute a great obstacle, as the UCTD establishes that any unnegotiated term which, "contrary to the requirement of good faith, […] causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer",[78] such as broad liability exemptions and exotic choices of forum and law, is deemed to be unfair and should not be enforced by courts. But for the rule to apply, it would be necessary to be in Europe or to have the law of a European country

[73] Mills (2024, 569–576); Infantino and Bussani (2024, 299–302).

[74] DSA, articles 4–6.

[75] Infantino (2022).

[76] On these issues, see Sect. 7.2.

[77] See above, note 73.

[78] UCTD article 3(1).

to apply to the claim. Let us therefore examine the conditions under which a claim against a company, including a digital service provider, for online abuse of digital vulnerability could be brought before European courts and the law under which it would be adjudicated.

Anyone considering suing a company after a digital accident would first need to identify and locate the defendant. Given the cross-border nature of the digital economy, the defendant may well be based outside Europe and have no European branch. This would not be good news for plaintiffs, as the general rule in transnational disputes is that a plaintiff can always sue a corporate defendant in the courts of the country where the defendant is headquartered. Yet, in order to protect consumers, EU conflict-of-law rules contain a special rule applicable to B2C relationships, according to which a consumer is entitled to bring an action against a company before the courts of the state where the consumer is domiciled, provided that the company pursues its commercial activities in that state.[79] This right cannot be waived by contract; any waiver or conflicting contractual provision designating a different exclusive forum is enforceable in Europe.[80]

Once the court of a European country has jurisdiction, the determination of the applicable law would follow the EU rules on private international law. These rules point to the "law of the country where the consumer has his habitual residence"[81] for contractual claims, to the "law of the country in which the damage occurs"[82] for tortious cases, and to the "law of the country in which the unjust enrichment took place" for unjust enrichment claims.[83] In most scenarios, the "country in which the damage occurs" and the "the country in which the unjust enrichment took place" would correspond to the country of residence of the plaintiff, therefore leading to the application of the law the plaintiff is more familiar with.[84] Claims brought in accordance with these rules may include cross-border representative actions.[85] Users residing in Europe, regardless the terms of use they agreed to, the location of the company they are dealing with, or the legal basis of the claim is, can bring their (individual and collective) private law claims against these companies before the courts and under the law of their country.[86]

Of course, none of the above would relieve the plaintiff of the need to prove all the requirements of the chosen cause of action under the applicable law and

[79] Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (BrusselsIbis), articles 6(1) and 18(1), as well as article 14.

[80] Regulation (EU) No 1215/2012 (n 79) article 19.

[81] Regulation (EC) No 593/2008 on the law applicable to contractual obligations (Rome I), article 6(1).

[82] Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II), article 4(1).

[83] Regulation (EC) No 864/2007, article 10(3).

[84] Van Dam (2021, 555, 571–572).

[85] Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers, article 6.

[86] Irrespective of the country involved, this law will likely be friendlier to consumers than any other: Infantino and Bussani (2024, 303–315).

to somehow avoid the application of possible defenses (such as the immunity of digital service providers under the DSA) that may be raised by the defendant. Overcoming the substantive, evidentiary, and procedural hurdles of the chosen cause of action under applicable law can be a significant burden. However, the presumption of digital vulnerability online and the possible application of a presumption of hyper-vulnerability may help in this regard.

A final point concerns the remedies available to the plaintiffs. The rules governing which remedies (e.g., invalidity of terms/contracts, performance, injunction, restitution, compensation) are available and under what conditions are largely determined by national private laws in Europe, which of course vary widely. European countries have remarkably different views on the range and extent of remedies that can be obtained through civil litigation. To fully protect against digital vulnerability, European courts would probably need to be creative and make generous use of the powers at their disposal to issue injunctions,[87] order the defendant to disgorge profits,[88] award non-patrimonial losses, especially in cases of serious violations of the duty to care about others' vulnerability and hyper-vulnerability,[89] and even grant ultra-compensatory awards, to the extent that this may be necessary to prevent the same conduct being repeated in the future.[90] After all, there are no rights without (adequate) remedies.

7.2 Peer-To-Peer Abuses

It would arguably be much more difficult to bring a claim for abuse of digital vulnerability against other individuals acting online. Such claims would face more hurdles than those against companies.

A first issue would be determining the legal basis for such a claim. In most cases, individuals who interact online, even if they do so through the same website, platform, or network, do not have a direct contractual relationship with each other. The terms and conditions users accept bind only the user and the website, platform, or network involved. Perhaps it could be argued that all subscribers to the same platforms are somehow part of the same contract, or that the contract with the platform obliges them to take into account the interests of relevant third parties, thus creating a contract with protective effects for third parties (i.e., other users). However, as far as we know, in all continental European legal systems to date, users are not considered to have a relationship with one another. This is not a problem in itself; all European legal

[87] For a plea about the use of injunctory relief (in the field of anti-discrimination), Halberstam and Van Den Bogaert (2023).

[88] For such a possibility, see Lee (2026).

[89] European jurisdictions adopt a variety of approaches with regard to non-patrimonial damages: de Conca and Infantino (2024); Li (2023).

[90] National European laws exclude overt punitive damages awards, even though punitive considerations may creep into tort law through other devices: see Infantino and Wang (2019, 357–358).

systems have rules on non-contractual obligations (such as tort and unjust enrichment, as well as anti-discrimination and data protection) that can apply to everyone.

Yet, difficulties would lie elsewhere. First of all, a person interested in filing such a complaint would need to identify the possible defendants. Since most people operate online using nicknames, avatars, and pseudonyms, their true identity remains unknown to anyone other than the website, platform, or network where the interaction takes place. Moreover, many people have multiple online identities or accounts; at the same time, many online identities or accounts do not correspond to a real person. Anyone wishing to sue other users would first need to obtain information about the real-world identities of those users, which in many cases would mean requesting such information from the relevant website, platform, or network. If the company refuses, the plaintiff will have to seek a court order for disclosure.[91]

Secondly, assuming that such information is obtained, there remains the problem of identifying the competent courts to hear the claims and the law applicable to those claims. The difficulty here stems from the fact that peer-to-peer abuse of digital vulnerabilities often involves people who are resident or domiciled in different locations. In the Khelif case mentioned above in Sect. 4, the individuals who retweeted, posted, and reposted comments against her came from all over the world. This truly complicates the issue whenever the defendants in these transnational cases are located outside the EU, as jurisdiction over non-EU defendants extends beyond the scope of the EU's unified regime of private international law and, therefore, must be determined by the national law of the forum (whether intra- or extra-EU).[92]

Especially in cases of mass harms, where many people have contributed to the realization of the abuse, this can lead to a considerable problem of coordinating international actions.[93] The solution may be more manageable if claims can be brought against individuals domiciled in EU countries. The general rule for grounding jurisdiction in ordinary civil cases is that people domiciled in a EU MS may be sued in the courts of that state.[94] However, alongside this rule, there are special provisions for claims regarding non-contractual obligations, which state that persons domiciled in one MS may be sued in another MS "in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur".[95] In addition, article 8 of the Brussels Ibis Regulation provides that a person domiciled in a MS may also be sued "where he is one of a number of defendants, in the courts for the place where any one of them is domiciled, provided the claims are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings".[96] Given the risk that individual users may be impecunious and judgment-proof, it would seem prudent

[91] Infantino and Bussani (2024, 297).

[92] On the problems related to determining jurisdictions against non-EU defendants, Lutzi, Piovesani, Zgrabljić Rotar (2023, 21–26).

[93] Infantino and Wang (2019, 343–344).

[94] Regulation (EU) No 1215/2012 (n 79) article 4(1).

[95] Regulation (EU) No 1215/2012 (n 79) article 7, no (2).

[96] Regulation (EU) No 1215/2012 (n 79) article 8, no (1).

to base jurisdiction in the country where the defendant with the deepest pockets is domiciled. Whenever jurisdiction is established in one or more EU states, it is relatively straightforward to identify the applicable law. As we have already mentioned, the Rome II Regulation on the law applicable to non-contractual obligations stipulates that the law of the country where the damage or unjust enrichment occurred is applicable, which in most cases will be the country where the plaintiff resides.[97]

Assuming that the jurisdiction of a European court and the applicability of a European law are established, the plaintiffs would still have to prove the elements of the cause of action. For instance, in a fault-based liability claim, the plaintiff would have to prove the breach by the defendants of the applicable standard of care, the damage suffered, the causal link between the negligence of the defendants and that injury, the extent of the damages, and other technicalities depending on the law applicable to the action; in most cases, the plaintiff would also have to bypass the defense that the defendants were exercising their constitutionally protected freedom of opinion.[98] Many of these requirements may prove to be serious hurdles. While plaintiffs may find some support in the presumption of digital vulnerability, they may still find it difficult to persuade a court that their protection is more worthy than protecting the defendant's right to speak.[99] The same reasoning applies to proving the defendants' fault: if it is true that the duty to take care of the digital vulnerability of others depends largely on each person's ability to understand and protect the vulnerability of others, it would be up to the plaintiffs to prove that the defendants owed them a duty of care because of their experience, visibility, or authority.[100] Proof of damage can also be a problem, especially in cases of purely economic or non-economic losses, as many European legal systems are conservative in their approach to recovery in such cases.[101] But perhaps the most daunting problem would be proving causation. Particularly in cases where a number of people were involved in the act, the scenario would be one of cumulative causation, where each defendant contributed to the ultimate harm in some minimal way, and the extent of that contribution cannot be determined with precision.[102] To take the Khelif case again, it can hardly be said that the contribution of each of the people who retweeted the comments against her was a 'but-for' factor or a *condicio sine qua non* cause of the ultimate harm. European courts would have to be creative to solve this problem. They have been so in the past: for example, in similar minimal causation scenarios (such as toxic torts and environmental damage), European courts have often been able established causation in multi-defendant cases on the basis of the likelihood of causation.[103] Of course, in determining exactly who should be responsible for what, an assessment of each defendant's ability to understand and prevent the abuse should be made, so that

[97] See Regulation No 864/2007 (Rome II), articles 4(1) and 10(3); see also above, Sect. 7.1.

[98] Also on this point see Tsomidis (2022).

[99] See above, note 68.

[100] On this point, Bussani, Sebok, Infantino (2022, 27–42).

[101] See above note 89.

[102] Infantino and Zervogianni (2017, 652–653).

[103] See Infantino (2022); Infantino and Zervogianni (2017, 646–647).

causation and liability can be articulated taking into account each defendant's status and authority, their proximity to the victim, their role in the abuse, the severity and gravity of the attack, the number of people involved, and so on.[104] In particular, such an assessment should take into account the *interdependence of digital vulnerability* as highlighted in Sect. 3 above: since everyone is at once vulnerable to (corporate abuse as well as to) other people's attacks and empowered to attack other digitally vulnerable people, the extent to which people can be held accountable depends on the relational positions and capabilities of the people involved. As the old saying goes, bad people should pay, and very bad people should pay more.

8 Conclusions

We can imagine concerns that the world we describe could become a world of over-compensation. We do not believe this is the case. Even if claims arising from abuses of people's digital vulnerability could technically be brought before European courts and adjudicated under European private law, significant hurdles remain to making this litigation a reality. In addition to the well-known social, psychological and economic factors that reduce people's willingness to assert their rights,[105] abuses of digital vulnerability present additional hurdles that are typical of any cyber tort case. The transnational nature of the case, the immunities protecting digital service providers and users, the multiplicity of defendants and their possible anonymity, the difficulty of proving the elements of the cause of action, and the challenge of obtaining an adequate remedy are all factors that increase the difficulty of securing justice. Much would have to change for this litigation to open the floodgates of liability.

Yet, change is needed. In particular, it is essential to bring the legal framework closer to reality, namely that we live in hyper-connected societies in which all of us, except perhaps a minimal fraction, have very little understanding of the digital infrastructure in which we are immersed and on which we depend, and, in any case, have very limited means of protection. In a highly unbalanced context such as the digital environment, there is an urgent need to find some mechanisms and instruments that can somehow rebalance the existing power relations. We argue that this could be achieved by recourse to existing private law rules and remedies, as well as by changing the interpretation of individuals' status in the digital environment. Rather than clinging to the traditional view of the average online user, who is expected to assume all risks of harm simply by formally accepting standard terms and conditions and the availability of information that that they have never read, it would be more accurate to acknowledge that average online users are unaware of and exposed to risks that they never understood or accepted. In other words, it is necessary to

[104] When, for instance, the content is clearly sensitive and the speaker is authoritative and powerful, there may be heightened duties to behave correctly: on similar lines, see Fowler, Helveston, Robinson (2025).

[105] For the relevant literature, see Bussani and Infantino (2015, 83–90).

acknowledge that everyone online is digitally vulnerable, that many—particularly those at heightened risk of discrimination—are hyper-vulnerable, and that everyone operating in the online world, including individuals, should be mindful of the digital vulnerability experienced by other users and behave accordingly.

We have tried to demonstrate that the above change does not require any specific reform, but rather a shift in understanding and the interpretation of existing rules regarding private rights, obligations, and remedies. Of course, a similar shift could probably be brought about more easily if it were enacted through legislative reform, as has been done in Latin America. But we should bear in mind that, for centuries, much of the development of private law in Europe has depended on the creativity and courage of academics and judges to imagine the legal world not as it is, but as it could be.[106] As is often the case with revolutions, change depends on us all.

References

Balkin JM (2020) The fiduciary model of privacy. Harvard Law Rev 134:11–33
Bartl M (2015) Internal market rationality, private law and the direction of the union: resuscitating the market as the object of the political. Eur Law J 21(5):572–598
Ben-Shahar O, Porat A (2021) Personalized law. Different rules for different people. Oxford University Press, Oxford
BEUC (2021) EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets. Available at https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf
Bradford A (2023) Digital empires. The global battle to regulate technology. Oxford University Press, Oxford
Burk DL (2021) Algorithmic legal metrics. Notre Dame Law Rev 96:1147–1204
Bussani M, Infantino M (2015) Tort law and legal cultures. Am J Comp Law 63(1):77–108
Bussani M, Sebok AJ, Infantino M (2022) Common law and civil law perspectives on tort law. Oxford University Press, Oxford
Calabresi G (1985) Ideals, beliefs, attitudes, and the law. Private law perspectives on a public law problem. Syracuse University Press, Syracuse
Caruso D (2012) The "Justice Deficit" debate in EU private law: new directions. BU Law Working Paper (2012). Available at https://scholarship.law.bu.edu/faculty_scholarship/590/
Chamallas C, Wriggins JB (2010) The measure of injury: race, gender, and tort law. New York University Press, New York
Clément D (2018) Human rights or social justice? The problem of rights inflation. Int J Human Rights 22:155–169
Colombi Ciacchi A (2019) The direct horizontal effect of EU fundamental rights. Eur Const Law Rev 15(2):294–305
Crea C, De Franceschi A (eds) (2024) The new shapes of digital vulnerability in european private law. Nomos, Baden-Baden
Crenshaw K (1989) Demarginalizing the intersection of race and sex: a black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. Feminist Legal Theory 3(1):139–167
de Conca S, Infantino M (2024) A difficult puzzle: the duty of care in Member States' tort law and the GDPR. Datenschutz und Datensicherheit 48:566–571

[106] Merryman and Pérez-Perdomo (2007, 56–68); Sacco (1991), 346–350.

De Gregorio G (2022) Digital constitutionalism in Europe. Reframing rights and power in the digital society. Cambridge University Press, Cambridge
Domurath I (2024) Digital vulnerability as a power relation: hyper- and hypo-autonomy and why thick privacy matters. In: Crea C, De Franceschi A (eds) The new shapes of digital vulnerability in European private law. Nomos, Baden-Baden, pp 227–258
Endicott T, Young K (2022) The death of law? Computationally personalized norms and the rule of law. Univ Toronto Law J 72:373–402
European Commission (2024a) Study to support the Fitness Check of EU consumer law on digital fairness and the report on the application of the Modernisation Directive (EU) 2019/2161. Final Report—Part 1. Available at https://commission.europa.eu/publications/study-support-fitness-check-eu-consumer-law-digital-fairness-and-report-application-modernisation_en
European Commission (2024b) Commission Staff Working Document Fitness check of EU consumer law on digital fairness. SEC(2024) 245 final. Available at https://commission.europa.eu/document/download/707d7404-78e5-4aef-acfa-82b4cf639f55_en?filename=Commission%20Staff%20Working%20Document%20Fitness%20Check%20on%20EU%20consumer%20law%20on%20digital%20fairness.pdf
European Commission (2016) Consumer vulnerability across key markets in the European Union. Final report. Available at https://op.europa.eu/en/publication-detail/-/publication/79b42553-de14-11e6-ad7c-01aa75ed71a1
Fineman MA (2008) The vulnerable subject: anchoring equality in the human condition. Yale J Law Fem 20:8–40
Floridi L (ed) (2015) The onlife manifesto. Springer, Cham
Fowler LR, Helveston M, Robinson Z (2025) Influencer speech-torts. Georgetown Law J 113(3):45–103
Gellert R (2024) The digital vulnerable consumer: a concept with critical potential or entrenching logics of market efficiency. Available at https://transformativeprivatelaw.com/the-digital-vulnerable-consumer-a-concept-with-critical-potential-or-entrenching-logics-of-market-efficiency/.
Grochowski M (2024) Digital vulnerability in a post-consumer society. subverting paradigms?. In: Crea C, De Franceschi A (eds) The new shapes of digital vulnerability in European private law. Nomos, Baden-Baden, pp 201–227
Halberstam D, Van Den Bogaert S (2023) A fresh look at judicial remedies in EU equality law and beyond: The untapped possibility of structural injunctions. Common Market Law Rev 60(5):1269–1312
Hesselink M, Soei Len T (2025) European private law & intersectionality: three strategies. Eur Law Open 1–22
Infantino M (2025) Consumers' vulnerability. In: Micklitz H-W, Namysłowska M (eds), Consumer law encyclopedia. Edward Elgar. Cheltenham, forthcoming
Infantino M, Bussani M (2024) Tort law in the metaverse. In: diMatteo L, Cannarsa M (eds) Research handbook on the metaverse and law. Edward Elgar, Cheltenham, pp 292–309
Infantino M (2022) Causation in algorithmic torts. In: Belser EM, Pichonnaz P, Stöckli H (eds) Le droit sans frontières. Mélanges pour Franz Werro. Stämpfli, Berne, pp 375–384
Infantino M, Wang W (2019) Algorithmic torts: a prospective comparative overview. Transnatl Law Contemp Probls 28:309–623
Infantino M, Zervogianni E (2017) Summary and survey of the results. In: Infantino M, Zervogianni E (eds) Causation in European tort law. Cambridge University Press, Cambridge, pp 587–665
Kaplan Y, Gordon-Tapiero A (2024) Unjust enrichment by algorithm. George Wash Law Rev 92:305–358
Keats Citron D (2022) The fight for privacy. Protecting dignity, identity, and love in the digital age, Norton & Co., New York
Kohnt NA (2014) Vulnerability theory and the role of government. Yale J Law Feminism 26(1):1–28
Krämer L (2021) The origins of consumer law and policy at EU Level. In: Micklitz H-W (ed) The making of consumer law and policy in Europe. Hart, Oxford, pp 13–30

Lee C (2026) Beyond algorithmic disgorgement: remedying algorithmic harms. UC Irvine Law Rev 16
Lee E (2022) Virtual governments. UCLA J Law Technol 4:1–32
Lessig L (2006) Code and other laws of cyberspace, Version 2.0. Basic Books, New York
Li S (2023) Compensation for non-material damage under Art. 82 GDPR: a review of Case C-300/21. Maastricht J Eur Comp Law 30(3):335–345
Lutzi T, Piovesani E, Zgrabljić Rotar D (2023) Comparative report. In: Lutzi T, Piovesani E, Zgrabljić Rotar D (eds) Jurisdiction over non-EU Defendants. Should the Brussels Ia Regulation be Extended?. Bloomsbury, London, pp 3–28
Macioce F (2022) The politics of vulnerable groups. Implications for philosophy, law, and political theory, Springer, Cham
Mackenzie C (2013) The importance of relational autonomy and capabilities for an ethics of vulnerability. In: Mackenzie C, Rogers W, Dodds S (eds) Vulnerability. New essays in ethics and feminist philosophy. Oxford University Press, Oxford, pp 33–59
Malgieri G (2023) Vulnerability and data protection law. Oxford University Press, Oxford
Malgieri G, Niklas J (2020) Vulnerable data subjects. Comp Law Secur Rev 37:105415. Available at https://www.sciencedirect.com/science/article/pii/S0267364920300200
Martínez Alles MG (2025) Reducing inequality in consumer transactions: the significance of aggravated vulnerabilities. In: Davis KE, Pargendler M (eds), Legal heterodoxy in the global south: adapting private laws to local contexts. Cambridge University Press, Cambridge, pp 77–111
Mercosur (2021) Resolution no 11/2021. Protección al consumidor hipervulnerable. Available at https://normas.mercosur.int/public/normativas/4116
Mercosur (2019) Resolution no 36/2019. Consumidores en el mercado. Available at https://normas.mercosur.int/simfiles/normativas/73866_RES_036-2019_ES_Defensa%20Consumidor%20Principios%20Fundamentales.pdf
Merryman JH, Pérez-Perdomo R (2007) The civil law tradition. An introduction to the legal systems of Europe and Latin America. 3rd edn, Stanford University Press, Stanford
Micklitz H-W et alii (2024) Towards digital fairness. J Eur Consumer Market Law 13:24–30
Mills G (2024) A contractual approach to social media governance. Yale Law Policy Rev 42:522–625
Pistor K (2019) The code of capital: How the law creates wealth and inequality. Princeton University Press, Princeton
Riefa C (2022) Protecting vulnerable consumers in the digital single market. Eur Bus Law Rev 33:607–634
Sacco R (1991) Legal formants: a dynamic approach to comparative law (installment II of II). Am J Comp Law 39:343–401
Schulze R, Staudenmayer D (eds) (2024) EU Digital Law. Beck, Munich
Smits JM (2014) Contract law. A comparative introduction. Edward Elgar, Cheltenham
Teubner G (2006) Coincidentia oppositorum: hybrid networks beyond contract and organization. In: Gordon R, Horwitz M (eds) Law, society, and history: themes in the legal sociology and legal history of Lawrence M. Friedman. Stanford University Press, Stanford, pp 367–394
Theilen JT (2021) The inflation of human rights: a deconstruction. Leiden J Int Law 34(4):831–854
Tsomidis T (2022) Freedom of expression in turbulent times—comparative approaches to dangerous speech: the ECtHR and the US Supreme Court. Int J Human Rights 26:379–399
van Dam C (2021) Transnational tort law. In: Zumbansen P (ed) The oxford handbook of transnational law, 2nd edn. Oxford University Press, Oxford