CONCLUSIONS

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

Digital Vulnerability in European Private Law – Conclusions

Reiner Schulze

A. Introduction

The discussions at the conference in Ferrara[1] which are documented in this volume impressively demonstrate the weight and diversity of the challenges that digital vulnerability poses for European Private Law in the face of new technological developments.[2] This vulnerability can affect individuals in many different situations and functions – be it as consumers or other market participants, be it in their education or in their professional activities as employees, business founders or entrepreneurs, or be it in their leisure time or retirement. Against the background of the variety of digital vulnerabilities and possible legal responses discussed, just a few overarching points of view can be emphasised below in order to provide suggestions for further reflection on the tasks of jurisprudence, legislation, and case law in this area:

- the importance of digital vulnerability as a challenge for European private law
- the character of this topic as a cross-cutting social and legal issue
- some approaches to legal responses based on both traditional protection instruments and new concepts

B. A new challenge for European Private Law

As far as the significance of the topic of 'digital vulnerability' for 'European Private Law' is concerned, the contributions in this volume and the confer-

1 Digital Vulnerability in European Private Law, Conference in Ferrara on 15 and 16 June 2023.

2 On the challenges posed to European Private Law by these technological developments see Reiner Schulze, 'European Private Law in the Digital Age – Developments, Challenges and Prospects' in André Janssen, Matthias Lehmann and Reiner Schulze (eds), *The Future of European Private Law* (Nomos 2023) 141 ff.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

ence on which they are based vividly demonstrate the close links between the two concepts in many facets. Certainly, the project of the internal market, which today includes the 'Digital Single Market'[3], has been at the centre of European integration from the very beginning. But the EU's ambition has always been to combine – and to some extent balance – this orientation of integration with regard to the market with the protection of the weaker affected by structural disadvantages and/or particular vulnerability – for example, protection against discrimination on grounds of gender or origin; appropriate social protection including protection of workers; consumer protection. This synthesis of internal market development and protection of the vulnerable is reflected in many measures of EU legislation; among other things in its directives against discrimination[4] and on labour law[5], and not least in its highly developed consumer law.[6] With the transition to the digital age, not only the further development of the internal market into the 'Digital Single Market' has accordingly become necessary, but also the further development of protection policies with regard to the consequences of digitalisation, and this includes protection with regard to digital vulnerability. In other words, both the development of the Digital Single Market and protection against digital vulnerability together pose challenges for the EU and for the development of European law in the digital age.

These challenges for European law are not limited to measures of a public law nature but also include areas of private law. In the early days of the European Communities, European legislation focussed on public law. However, since the 1960s it has increasingly extended to matters of private law. In the course of this development, the term 'European Private

3 Commission, 'A Digital Single Market Strategy for Europe' (Communication) COM (2015) 192 final.

4 Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L 180/22; Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation [2000] OJ L 303/16; Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services [2004] OJ L 373/37; Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) [2006] OJ L 204/23.

5 For an overview see Gregor Thüsing, *European Labour Law* (CH Beck 2013).

6 For an overview see Geraint Howells, Christian Twigg-Flesner and Thomas Wilhelmsson, *Rethinking European Consumer Law* (Routledge 2018).

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

Law' has come to be used for the law that the European Communities and later the EU have created for these matters (as one variant of this term alongside others which include commonalities of national laws in Europe which exist independently of EU law).[7] In this sense, European Private Law is today of crucial importance in many respects both for the functioning of the internal market and for the EU's protection policies. This is reflected in numerous legal acts ranging from non-discrimination (e.g. with regard to equal treatment in the supply of goods and services[8]) to social policy (inter alia with regard to labour relations) and the protection of small and medium-sized enterprises (e.g. with regard to legal relations between self-employed commercial agents and principals[9] or with regard to late payment in commercial transactions[10]) to consumer protection (through a variety of legal acts such as the Unfair Terms Directive[11] and the Consumer Rights Directive[12]). In this respect, the understanding and legislative practice of European private law differs profoundly from the older concepts of private law, which at the end of the 19th century were characterised in some European countries by the then prevailing understanding of liberalism and originally formed the basis of their codifications.

It is therefore not only the digital age that has given rise to the desire to incorporate the protection of the weak and vulnerable into the concept of European private law. However, the technological, economic, and social

7 Reiner Schulze and Fryderyk Zoll, *European Contract Law* (3rd edn, Nomos 2021) ch 1 mn 13ff.

8 Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L 180/22 (in particular art 3 para 1 lit h) and Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services [2004] OJ L 373/37.

9 Council Directive 86/653/EEC of 18 December 1986 on the coordination of the laws of the Member States relating to self-employed commercial agents [1986] OJ No L 382/17.

10 Directive 2011/7/EU of the European Parliament and of the Council of 16 February 2011 on combating late payment in commercial transactions (recast) [2011] OJ L 48/1.

11 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ No L 95/29 (Unfair Terms Directive).

12 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L 304/64 (Consumer Rights Directive).

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

changes resulting from digitalisation pose new challenges in terms of substantiating and effectively implementing this aim.

EU legislation has already taken the first steps in this direction.[13] A striking example is provided by the most recent legal acts on the further development of consumer protection with regard to the changes brought about by digitalisation, in particular the 'twin directives' of 2019, which concern contracts for digital content and services as well as consumer purchases, including the purchase of goods with digital elements.[14] The same applies, for example, to the provisions relevant to private law in the Digital Services Act, which is also intended to safeguard the principle of consumer protection and other fundamental rights in the online environment[15], or for the adaptation of product liability to the changes resulting from digitalisation.[16] These examples also show that the EU is addressing the new tasks in both of the main forms of its legislation: by harmonising the laws of the Member States through directives and, increasingly, by creating directly applicable uniform European law through regulations.[17] Beyond this recent legislation, which primarily relates to the European Commission's 'Digital Single Market Strategy' of 2015[18], the question now arises as to whether and, if so, in what way the new phenomenon of digital vulnerability requires the conceptual and legislative design of European private law to be further developed specifically with regard to this challenge.

13 Denise Amram, 'Standards to Face Children and Patients Digital Vulnerabilities', in this volume. For an overview see also Schulze and Zoll (n. 7 above) ch 1 mn 61ff.

14 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1 (Digital Content Directive) and Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L 136/28. On the effect of this Directive on the law of the member states see Alberto De Franceschi and Reiner Schulze (eds), *Harmonizing Digital Contract Law* (CH Beck - Hart - Nomos 2023).

15 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 [2022] OJ L 277/1 (Digital Services Act - DSA), art 1 para 1.

16 See Commission, 'Proposal for a Directive of the European Parliament and of the Council on liability for defective products' COM (2022) 495 final (newly drafted Product Liability Directive). See also Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Liability for AI* (vol VII of the series 'Münster Colloquia on EU Law and the Digital Economy', Nomos 2023).

17 Schulze (n. 2 above) 145.

18 See n. 3 above.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

C. Concept and cross-cutting nature of digital vulnerability

As far as the challenges associated with the term 'digital vulnerability' are concerned, numerous and very different areas of life and therefore also many legal matters need to be taken into consideration. This is all the more true when one considers the breadth and depth to which the use of Artificial Intelligence in particular is already affecting society and the everyday lives of individuals and will continue to do so in the future. The broad scope and diversity of the consequences of digitalisation therefore preclude attributing 'digital vulnerability' to a single specific risk situation or a single type of potentially harmful actions. Rather, research in this field will have to consider different types and causes of such vulnerability (or of such 'vulnerabilities'[19]) and different concepts of 'vulnerability' in the digital world.[20]

However, despite this diversity, a common characteristic of the situations covered by this term is likely to be that the use of digital technologies contributes to creating or increasing the risk of harm to the rights or interests of a person or group of persons, in whichever of the many different contexts of digital communication and the use of digital content these risks may arise. One outstanding example is the wide range of risks resulting from the use of digital devices making personal data available to others or allowing others access to such data. In this respect, the challenges with regard to digital vulnerability overlap with data protection concerns[21] and with the regulation of trade in data under public and private law.[22] Not least, the question of a need for protection as a result of digitalisation may arise, for example, in situations in which the user of a digital device or digital services is dependent on the use of Artificial Intelligence and information process-

19 Federica Casarosa and Hans-W. Micklitz, 'Addressing Vulnerabilities in Online Dispute Resolution', in this volume.

20 Niti Chatterjee and Gianclaudio Malgieri, 'The Metaverse and Consumers' Vulnerabilities', in this volume.

21 Fundamentally, see 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 [2016] OJ L 119/1 (General Data Protection Regulation - GDPR).

22 In recent implementation, see Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 OJ L Series 22.12.2023 (Data Act); e.g. also art 3 of the Digital Content Directive with regard to the provision of personal data as counter-performance.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

ing that is beyond his or her control.[23] This dependency can give rise to a variety of risks that can be considered a specific result of digitalisation (in its advanced form of the use of Artificial Intelligence).

In some situations, however, it may prove more difficult to distinguish 'digital risks' from threats that exist independently of a digital context and to assess whether the digital context has increased or even reduced vulnerability. For example, if consumers use artificial intelligence when concluding an online purchase contract, this use may compensate them for some of the disadvantages in terms of information asymmetry vis-à-vis the commercial seller. On the other hand, however, they become dependent on the artificial intelligence provider as mentioned above (who may even act on behalf of both parties to the purchase contract in the case of a machine-to-machine purchase). Whether in these situations the digitalisation of the conclusion of the contract has ultimately improved the position of the consumers or increased the risk of their vulnerability may vary depending on the circumstances of the individual case and is generally difficult to assess. Careful consideration is likely to be required in order to arrive at a typification of vulnerability in such cases and to further develop the provisions on consumer protection when concluding contracts on this basis.

But even beyond this, it seems doubtful to use the concept of digital vulnerability for all situations in which new risks arise with regard to material or immaterial goods as a result of digital technologies and to assume that the persons affected always require legal protection in such situations. Rather, it will first have to be considered to what extent the affected parties themselves are fundamentally able to protect their interests, also with regard to such new situations, within the framework of private autonomy. If this is not the case (for example, because a structural imbalance between the parties or similar structural circumstances in the legal relationship in question make it difficult for one party to effectively protect its interests), legal measures may be necessary to protect against the consequences of digitalisation (for example, general provisions such as those adopted for the protection of natural persons with regard to the processing of personal data in the GDPR[24] or for the protection of injured parties with regard to the

23 Teresa Rodríguez de las Heras Ballell, 'Digital Vulnerability and the Formulation of Harmonized Rules for Algorithmic Contracts: A Two-sided Interplay', in this volume.

24 See n. 21 above.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

liability of producers for software in the Product Liability Directive[25]). Such situations may be described as 'digital vulnerability' in a broad sense.

However, it remains to be considered whether a narrower understanding of the term is more appropriate alongside or instead of such a broad use. A narrower understanding of 'digital vulnerability' could be particularly suitable in view of the terminology that has already emerged, for example, in consumer law for the 'vulnerable consumer' (as opposed to the 'average consumer' or 'reasonable-circumspect consumer'[26]). In the corresponding understanding, 'digital vulnerability' would not cover the entirety of the risks that arise for everyone in the legal relationship in question as a result of digitalisation and that may require general legislative measures. Rather, the concept is limited to the additional risks that may arise as a result of digitalisation for certain individual groups of people due to special circumstances (for example, with regard to their social and professional situation and their stage of life). Even in this narrower understanding, however, 'digital vulnerability' covers a wide range of very different situations which clearly proves to be a cross-cutting issue in both respects: with regard to the factual circumstances to be taken into account and with regard to the legal matters to be included.

From a factual point of view, social circumstances in particular come into consideration, which can favour a specific vulnerability of groups of people through digitalisation. These include, among many other things, issues of education, income, and social role allocation, which can have a negative impact on the participation in digital communication, the ability to utilise information and the protection of one's own interests in the digital world for the groups of people concerned. Not least, with regard to the relevant factual circumstances, it must also be taken into account that digital vulnerability can be based on physical impairments and, in particular, often on specific problems in certain phases of life. In the latter respect, the cross-cutting theme of digital vulnerability ranges from 'child vulnerability'[27] (for example in relation to 'smart toys' for young children or to digitally produced and distributed forgeries of images and other digital bullying at school) to the exploitation of 'digital weaknesses' of old people. Such areas of digital vulnerability also show that both can be considered to

25 See n. 16 above.

26 See Howells, Twigg-Flesner and Wilhelmsson (n. 6 above) 6-7, 48, 70-73.

27 Alessandra Pera and Sara Rigazio, 'Let the Children Play. Smart Toys and Child Vulnerability', in this volume; Shabahang Arian, 'Vulnerability in the Age of Metaverse and Protection of the Rights of Users Under EU Law', in this volume.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

a considerable extent: not only the risks with regard to material losses but also risks with regard to serious immaterial damage.

Incidentally, even with death digital vulnerability does not end. The 'eternal memory' of the internet outlives the individuals and allows access to what they wanted to guard for themselves personally during their life.[28] And even more: the manipulative power of artificial intelligence can change posterity's image of him or her (literally and figuratively, for example, what he or she wrote or painted); in other words, post-mortem, so to speak, fiction takes the place of the real personality, without the person whose personality has been violated being able to defend himself or herself.

This diversity of different situations that can lead to digital vulnerability is reflected in the wide range of legal matters in which legislation and the application of legal provisions must respond to this challenge. In other words: The wide spectrum of digital vulnerability as a phenomenon that encompasses many areas of society in the digital age is reflected at the level of law as a cross-cutting challenge for almost all areas of law, branches of courts and disciplines of legal doctrine. Just as for national law, it is therefore necessary for European private law to look at the multiple types of digital vulnerability across the breadth of private legal relationships, taking into account the context of the respective branches of private law. These branches overlap to some extent with the areas mentioned above, which EU legislation has already addressed in the context of various protection policies. They comprise, for example, the consumer law[29] including the consumer insurance sector[30], the damage law[31] the rules on Unfair Com-

28 Edina Harbinja, 'Post-mortem privacy 2.0: theory, law, and technology' (2017) vol 31 International Review of Law, Computers & Technology 26, 33.

29 Fabrizio Esposito, 'Investigating Digital Vulnerability with Theories of Harms: A Methodological Proposal with Three Illustrations', in this volume; Emilia Mišćenić, 'Information, Transparency and Fairness for Consumers in the Digital Environment', in this volume; Catalina Goanta, Giovanni de Gregorio and Jerry Spanakis, 'Consumer Protection and Digital Vulnerability: Common and Diverging Paths', in this volume; Jura Golub, 'Digital Vulnerability of Consumers in the World of Smart Contracts - Is European Private International Law "Digitalized" Enough?', in this volume.

30 Piotr Tereszkiewicz, Katarzyna Południak-Gierz and Patryk Walczak, 'Digital Vulnerability of Insurance Consumers and Personalised Pricing of Insurance Products under GDPR and UCPD', in this volume.

31 Chatterjee and Malgieri (n. 20 above), in this volume.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

mercial Practices[32], the labour law with regard to the digital vulnerability of employees[33], the online dispute resolution[34], and the private international law.[35] For all these and other areas, research into private law is faced with the task of analysing the new problems that arise in the digital age with regard to digital vulnerability and considering appropriate solutions in the respective legal context.

In contrast to such analyses in the context of the respective area of law, it would probably be a less promising approach to try to detach all issues of digital vulnerability entirely from their particular legal contexts and assign them exclusively to a separate new legal field of 'digital vulnerability'. Essentially, such an approach would be just as questionable as the general assumption that 'digital law' as a whole is to be contrasted separately with the law of the 'analogue world' as an independent field of law (and possibly that lawyers will in future split into 'digital lawyers' and 'traditional analogous lawyers' instead of private law, public law, etc). It is not recognisable that such a blanket replacement and isolation of 'digital law' from the rest of the legal system would find a basis in the current and foreseeable future development of positive law at the European or national level.[36] It would also not improve the legal possibilities for protecting digitally vulnerable groups of people but would only lead to an unnecessary complication of the legal protection system. It therefore seems preferable to take into account, as far as possible, the specific context of each of these areas of law for the legal approaches to solving the problems that digitalisation has created with regard to digital vulnerability in the various areas of law and in this way to adapt the respective areas of private law to the new challenges.

D. Some approaches for legal responses to digital vulnerability

Although this search for legal responses to digital vulnerability is a relatively recent challenge, the research contributions on the areas of law just

32 Mateja Durovic and Eleni Kaprou, 'The New Concept of Digital Vulnerability and the European Rules on Unfair Commercial Practices', in this volume; Arian (n. 27 above), in this volume.

33 Isabelle Wildhaber and Isabel Laura Ebert, 'From Digital Vulnerability to Data Anxiety: The Situation of Employees in Digitally Permeated Workplaces', in this volume.

34 Casarosa and Micklitz (n. 19 above), in this volume.

35 Gérardine Goh Escolar, 'Addressing Digital Vulnerability through Private International Law', in this volume.

36 Schulze (n. 2 above) 159ff.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

mentioned already reveal a number of approaches to further developing European private law in this respect. They concern both the adaptation of conventional protection instruments to the changes resulting from digitalisation, and the development of new concepts specifically with regard to digital vulnerability. On the one hand, the potential of existing protection instruments is therefore under consideration. This concerns, for example, information obligations to compensate for information asymmetries on the internet, rights of withdrawal for online transactions, or mandatory regulations regarding the contractual conformity of digital products. On the other hand, the possibilities for expanding and supplementing them, for example, through specific protection instruments such as responsibilities of digital intermediary services or the use of appropriate technologies such as 'filters' to prevent certain types of interference, must also be considered. Considerations in both respects are set out in more detail in the contributions to this volume against the background of the needs for protection in question. In the following, only three general features will be emphasised with regard to the legal responses to digital vulnerability.

I. The multilevel dimension

Digital vulnerability proves to be a multi-level challenge in various respects, as the contributions in this volume reveal – not only with regard to the levels and ways in which digital vulnerability arises, but also with regard to the levels at which legal responses need to be developed. In the latter respect, it is not only the various levels within one legal system that are under consideration – the constitution, private law regulations, application of the law by courts, alternative dispute resolution, self-regulation through codes of conduct, etc. Rather, special consideration must be given to the fact that the digital revolution – and the digital vulnerability associated with it – represents a multilevel challenge due to its cross-border nature, also with regard to the relationship between the national law of an individual state, supranational law of the European Union and international law that goes beyond this.

In the relationship between these three levels, EU law as the middle level deserves particular attention. This focus on the European law reflects, on the one hand, the cross-border nature of digitalisation and its significance for the European single market. On the other hand, it is due to the fact that

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

global approaches to legal solutions that extend beyond Europe are desirable, but currently only appear possible to a very limited extent – partly due to the political differences between the home states of the 'global players' in the field of digitalisation, including different approaches to assessing the consequences of digitalisation.[37] It currently seems to be emerging that Europe is taking its own path with regard to legal responses to the consequences of digitalisation, in contrast not only to China, but also to the USA in some areas – from data protection (as regulated in the GDPR[38]) to market regulation (through regulations such as the DMA[39]; DSA[40]; Data Act[41]) to liability for digital products (as dealt with in the newly drafted Product Liability Directive and in the Commission's Proposal for the AI Liability Directive[42]). Nevertheless, even from this European perspective, the legal framework and possibilities for action that extend beyond Europe must be considered.

Of significance is a series of projects aimed at adapting international regulations to technological changes and the resulting new protection requirements. In view of the cross-border nature of digital transactions, the question arises in particular as to how the problem of digital vulnerability can be incorporated into the further development of private international law.[43]

However, this problem will also have to be taken into account in the endeavours towards international legal unification in its many forms, from conventions to model laws. This concerns, for example, UNIDROIT's projects with regard to the new technologies of the digital age. The work of UNCITRAL in this regard is likely to be no less significant, in particular its work on a possible adaptation of the international sales law to the changes

37 See Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Liability for Artificial Intelligence and the Internet of Things* (vol IV of the series 'Münster Colloquia on EU Law and the Digital Economy', Nomos 2019) 15-16.

38 N. 21 above.

39 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act - DMA).

40 N. 15 above.

41 N. 22 above.

42 Newly drafted Product Liability Directive (n. 16); Commission, 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)' COM (2022) 496 final.

43 Goh Escolar (n. 35 above), in this volume.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

brought about by digitalisation.[44] In the past, the Vienna Convention on the International Sale of Goods of 1980 has given lasting impulses to European contract law (in particular through its influence on the 'Principles of European Contract Law' of the Lando Commission[45] and on the Consumer Sales Directive of 1999[46]). With regard to the renewed modernisation of contract law, which appears necessary as a result of digitalisation at both European and international level, perhaps a mutual stimulation of the projects on both levels could be achieved. Innovations already achieved in EU legislation (e.g. in the Digital Content Directive with regard to updating obligations and the legal consequences of termination[47]) could provide inspiration for the further development of international sales law. Accordingly, the considerations on automated contracting with regard to international trade law[48] could provide impetus for preliminary considerations for European legislation on this topic[49] and lead to a mutually fruitful dialogue.

II. Interaction with public law

A significant feature of many efforts to find legal answers to the problems of digital vulnerability is the interplay between approaches under private and public law. This includes the legal basis for protection against such violations. Honour, other personal rights, and the property rights of the individual are among the rights that are traditionally protected by private law. However, they are also protected by fundamental rights[50] – at European level by the Charter of Fundamental Rights. This Charter is also of particular importance with regard to digital vulnerability in that it lays down the right to the protection of personal data (art 8) and consumer pro-

44 Rodriguez de las Heras Ballell (n. 23 above), in this volume.
45 Ole Lando and Hugh Beale (eds), Principles of European Contract Law (Parts I and II, Kluwer Law International 2000).
46 Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees [1999] OJ L 171/12. See also Dirk Staudenmayer, in Reiner Schulze and Dirk Staudenmayer (eds), *EU Digital Law* (Commentary, Nomos 2020) 109-110, 133-134; André Janssen, Matthias Lehmann and Reiner Schulze, 'The Future of European Private Law – An Introduction' in Janssen, Lehmann and Schulze (n. 2 above) 20.
47 Digital Content Directive, art 7 lit d, art 8 para 2, arts 16, 17.
48 Rodríguez de las Heras Ballell (n. 23 above) 246, 249, in this volume.
49 For example, the upcoming conference on 'AI-Contracting' in Münster, January 2025.
50 Amram (n. 13 above), in this volume.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

tection (art 38) in individual articles. On this basis, the EU has combined provisions that may be relevant with regard to digital vulnerability, both in terms of public and private law and sometimes in one set of rules (e.g. predominantly public law with regard to the protection of personal data in the General Data Protection Regulation, predominantly private law with regard to the purchase of digital products in the Digital Content Directive).

The analysis and further development of legal solutions with regard to the various types of digital infringements must therefore often take into account a possible tension between, on the one hand, assessments based on private law and, on the other, values embodied in the fundamental right concerned, for example, with regard to the role of private autonomy in contract law and the values of fundamental rights in the Constitution.[51] Accordingly, the question often arises as to whether public law measures such as bans on certain content on the internet or private law instruments such as the liability of users or intermediary services are preferable for legislation in the respective circumstances. In all such issues, the analysis of the causes and forms of digital vulnerability and the development of legal responses cannot be limited to the boundaries of the discipline of private law but must include public law perspectives.

III. Consumer protection and protection of Internet users

In addition to the multilevel dimension of digital vulnerability and the issues of the interplay between private law and public law, the relationship between consumer protection and the protection of internet users has proven to be a third overarching topic of particular relevance. In this respect, it is not only becoming apparent that the challenges of protecting against digital vulnerability are to a large extent issues of consumer protection. Rather, the question also arises as to whether and to what extent, on the one hand, consumer protection should be extended with regard to the protection of Internet users in the face of digital vulnerability and, on the other hand, the protection of Internet users in the face of digital vulnerability should be a new and broader approach alongside or in place

51 See, for example, Goanta, de Gregorio and Spanakis (n. 29 above) 29, in this volume (with reference to Evelyn Douek, 'Content Moderation as Systems Thinking' (2022) 136 Harvard Law Review 526).

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

of conventional concepts of consumer protection[52] – pointedly put: user protection instead of consumer protection.

Numerous recent research studies and correspondingly multiple contributions in this volume have emphasised the first-mentioned aspect by addressing requirements and approaches for the further development of European consumer law. This concerns overarching considerations on the implications of digital vulnerability for EU consumer law[53] as well as a number of individual aspects. These range, for example, from the gap between digital fairness and transparency in EU Consumer Law[54] to the digital vulnerability of insurance consumers with regard to personalised pricing of insurance products. The same applies to the further development of European private international law with regard to the 'digital vulnerability of consumers in the world of smart contracts'.[55]

Nevertheless, the concept of consumer protection does not provide a sufficient framework to comprehensively analyse the problem of digital vulnerability and to develop approaches for legal responses in their full scope. This was already evident in the structure of the conference from which this volume emerged: While the digital vulnerability of the consumer is explicitly mentioned in the title of two of its sections, another section broadens the perspective to include 'users protection'. This indicates that the discussions on digital vulnerability and the approaches to legal protection measures in this respect are in a tense relationship between the traditional concept of consumer protection on the one hand and the focus on the protection of Internet users (or at least users of certain forms of digital communication) on the other. The question of user protection in addition to consumer protection arises here in particular because Internet users are exposed to digital vulnerability in numerous situations in which they are not protected as consumers in the traditional understanding of EU law (for example, in the case of infringements caused by persons or institutions other than traders or by traders with whom they have not entered or do not wish to enter into a legal relationship). In such situations, it is likely to be difficult to further

52 Reiner Schulze, 'Quelles limites aux droit de la consommation? - Propos introductifs' in Gerald Mäsch and others (eds), *Quelles limites aux droit de la consommation?* (forthcoming).

53 Irina Domurath, 'Digital Vulnerability as a Power Relation: Hyper- and Hypo-Autonomy and why Thick Privacy Matters', in this volume; Esposito (n. 29 above), in this volume.

54 Mišćenić (n. 29 above), in this volume.

55 Golub (n. 29 above), in this volume.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

develop the protection of those affected with regard to the risks posed by new technological developments on the basis of the current understanding of the consumer in EU law. It is therefore necessary to reconsider whether and to what extent, in view of these developments, another concept – such as that of the 'user' – should take over or at least supplement the current role of the consumer concept.

This issue of the relationship between the concept of consumer and the concept of user is expressed, for example, in the considerations focussing on the topic of digital vulnerability in the 'post-consumer society'[56] and in the critical reflections on personalised pricing and the notion of consumer with regard to individual traditional areas of consumer protection, such as the consumer insurance sector.[57]

E. Further tasks for legislation and research

The concept of the user also draws attention to another dimension of digital vulnerability: Internet users can digitally harm other people – for example by spreading photos and fake news or through other forms of bullying on social media – even in situations in which these others do not use the Internet. Such violations by internet users can affect high-ranking rights such as human dignity and other personal rights and can be directed against both individuals and groups of people (e.g. with regard to their ethnic origin, religion, or sexual orientation), regardless of whether they themselves are users of the internet at all. In this respect, not only the protection of users but also the protection against users can be of considerable importance with regard to digital vulnerability. Accordingly, it must be taken into account that the understanding of digital vulnerability should not only focus on the user as a potential victim of the violation but also independently of this on the user of digital media as a potential violator of the rights and legitimate interests of others.

Furthermore, with regard to such situations, the structures of communication on the Internet must be taken into account, and therefore the role of intermediary services of various kinds (such as mere conduit services,

56 Mateusz Grochowski, 'Digital Vulnerability in a Post-Consumer Society. Subverting Paradigms?', in this volume.

57 Tereszkiewicz, Południak-Gierz and Walczak (n. 30 above), in this volume.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -

caching services, and hosting services[58]) must be included in addition to the users from whom an infringement originates and the victims of the infringement (both users and non-users). Such intermediaries are to a certain extent transmission belts of the digital infringement. Depending on the circumstances, they may significantly increase the impact of the infringement due to the nature and extent of the distribution of the digital content concerned. In this respect, too, it is clear that the problem of digital infringement cannot be understood as a simple two-person relationship between an Internet user and another user. Rather, the understanding of digital vulnerability must take into account the specific complexity of the structures of digital communication; and the legal solutions must also take into account the specific nature of these structures.

EU legislation has now addressed such special features of digital communication with legal acts such as the Digital Services Act. With this legal act, it has taken particular account of the prominent role of intermediary services in the daily lives of EU citizens[59] in order to effectively protect fundamental rights, as provided for in the Charter of Fundamental Rights, in addition to the functioning of the internal market (art 1 para 1 DSA). The protection extends, among other things, to the dissemination of manifestly illegal content and unfounded notices and complaints (art 23 DSA) and to the privacy, safety, and security of minors (art 28 DSA). The legal act uses new instruments such as the responsibility of intermediary services and combines public law protection mechanisms with private law options for action such as individual claims for damages (art 54 DSA).

In this way, the Digital Services Act contains important and, in some cases, innovative approaches to countering serious forms of digital vulnerability such as the dissemination of illegal content and unsubstantiated messages. It can therefore be seen as one of the first moves with which EU legislation has set out to develop legal responses to the problem of digital vulnerability. As the articles in this volume show, there are evidently many more tasks for legislation and academic research to tackle along the way.

58 As defined in the Digital Services Act, art 3 lit g.
59 See Digital Services Act, recital 1.

https://doi.org/10.5771/9783748940913-521 https://www.inlibra.com/de/agb - Open Access -