Giorgia Guerra

Redesigning Protection for Consumer Autonomy

The case-study of *dark patterns* in European private law

DIRITTO E SOCIETÀ

FrancoAngeli

Giorgia Guerra

Redesigning Protection for Consumer Autonomy

The case-study of *dark patterns* in European private law

DIRITTO E SOCIETÀ

FrancoAngeli

This book was funded by the National Excellence Project on the topic "Law, Changes and Technology", won by the Verona Department of Law (2018-2022).

The volume underwent a double-blind peer review process to ensure a fair and transparent critical assessment.

Isbn: 9788835154839

INDEX

II. When autonomy struggles with *dark patterns*: promises and pitfalls of the current EU regulatory patchwork

III. Redesigning taxonomies and legal models of EU private law to protect the right of autonomy in the digital environment

AUTHOR'S ACKNOWLEDGEMENT

My interest in consumer law, policy and behaviour when involved in technological change dates back to 2003, when I started my PhD. Over the years, I had numerous chances to analyse the multi-faceted issue in the privileged field of law and converging technologies through the lens of comparative methodology.

I have many debts of gratitude for this. The most significant is to Prof. Marco Torsello, to whom I am grateful for having enrolled me into the vibrant academic community of the University of Verona, and for offering me the opportunity to work with him.

This book also benefited from valued insights. For all the constructive comments on the first draft of the book, I am particularly thankful to the professors I mention as follows in alphabetic order: Mateusz Grochowski (Max Planck Institute in Hamburg); Erica Palmerini (University Sant'Anna of Pisa); Cristina Poncibò (University of Torino); Karin Sein (University of Tartu); Filippo Viglione (University of Padova)1. I also wish to sincerely thank the anonymous reviewers for their helpful suggestions, which, ultimately improved the quality of manuscript. Remaining errors are my own.

Moreover, two visiting research periods, at the Centre of European Private Law of the University of Münster (2022) and at the Hamburg Max Planck Institute for Comparative and International Private Law (2023) contributed to making my ideas on the topic clearer, and to enrich the final work. Academic networks for exchanging ideas and getting feedback were invaluable players for my research.

Lastly, special thanks go to Mrs Kathryn Thoirs for her proof-reading support.

To my beloved mom, always with me

INTRODUCTION

Autonomy is an inherent aspect of consumer choice in Western legal traditions: its protection is at the core of fundamental issues of private law, particularly contract law.

A diachronic perspective on the concept of autonomy easily demonstrates that it is still a recurring topic in legal debates because novel research inquiries have emerged with data-driven technological innovation, where data-subjects victims of manipulation are often consumers. Indeed, today, the notion of the consumer as a weaker party is no longer the leitmotiv in the field; instead, the fact of rapid digitalisation in contemporary market structure has profoundly transformed the fundamental paradigm of liberal democracy, namely autonomy, whereby marketers have been granted a license to influence consumers, provided they protect their rights. Digital consumer behaviour shapes major legal concerns in business-to-consumer transactions and has spurred a growing interest in the topic from legal and social scholars.[1] For this reason, consumer autonomy deserves new intellectual efforts at European and transnational levels.

Commonly, consumers exercise autonomy whenever they freely choose from a set of possible options, though it is inevitably subject to constraints (e.g., price, time, information). However, only recently, social and economic studies, with a prominent role in behavioural law and economics, sough to explain how data-driven technologies nudge consumer self-determination, profiting from cognitive characteristics exploited by digital architectures.

The core idea of this book is, indeed, centred on the pivotal role that IT design can play in protecting fundamental rights, such as autonomy.

[1] Stefan Grundmann, Wolfgang Kerber, Stephan Weatherill (eds.), *Party Autonomy and the Role of Information in the Internal Market* (De Gruyter 2012) 3-38.

The problematic landscape considered is the following. In an over-informed society, everything is performed by algorithm-driven systems. Automation is critical to managing complexity, performing mass activities at an affordable cost, and ensuring effectiveness in processing data, information, and digital content. How Big Data analytics and artificial intelligence could change the nature of legal inquiries related to autonomy will undoubtedly act as the guiding light for this study. Ultimately, algorithms select and present digital content, impacting on consumer rights in several ways. The intensive and extensive use of algorithms has served a growing variety of tasks and activities and impacts on decision-making processes.

Algorithms and digital architectures can expose consumer (cognitive) vulnerabilities, known as digital vulnerability.[2]

Consumers can encounter advantages and costs due to sharing their data because some nudges are benign, while others deceive or steer them.

Notably, to illustrate how technology could, empirically, enhance or constrain consumers' autonomy, this book considers a specific case-study: the phenomenon of dark patterns, digital techniques designed to eradicate consumer consent and manipulate consumer self-determination.

Dark practices exploit cognitive vulnerabilities, which affect data subjects' autonomy and lead to lower quality choices. These tactics can originate from different practices, maliciously triggered, or stimulated by controllers: default settings, bait and switch, sneak into basket, disguised advertising interfaces, forced continuity or design choices that make price comparison more difficult and marketing practices discriminatory.

Specifically, dark patterns nag, trick, or manipulate consumers into buying products or services or giving up their privacy.

A screening ('sweep') on dark patterns commissioned by the European Commission and published in 2022 found that '97% of the 75 of the most popular websites and apps used by EU consumers deployed at least one dark pattern and the most prevalent were (1) hidden information/false hierarchy, (2) preselection, (3) nagging, (4) difficult cancellations, and (5) forced registration'.[3]

[2] Klaus Wertenbroch, Rom Y. Schrift, Joseph W. Alba, *et al*, 'Autonomy in consumer choice' (2020) 31 Mark Lett 429-439. Please refer to Chapter III.

[3] The screening is conducted on retail websites. It operates as a two-step action process: comprising screening websites to identify breaches of consumer law in a given online market; and enforcing traders, through national

While there has been some initial research on dark patterns in computer science and legal studies, their findings are primarily descriptive.[4] There is, in fact, no research that clarifies how consumers respond to dark patterns or examines the consequences of these tactics for consumers, companies, and society at large.[5]

The actual scope of the book is along the same line of reasoning currently shown by public authorities and institutions which have been asked to investigate if data-driven technologies respect or, on the contrary, undermine consumers' autonomy and to what extent traditional legal categories are still effective. The nature of the right to autonomy involves critical reflection on the distinction between traditional concepts of autonomy, and personal freedom – such as the classic one developed by Hobbes in Leviathan – which poses the ability to act on and satisfy one's personal preferences at the core of what autonomy is, and the perceived autonomy that social media filter-bubbles and digital choice architectures could enhance, which is threatened by cognitive bias.

Analysing the evolving concept of autonomy facing the problem of dark patterns, requires leaving aside the traditional narrative, which is rooted in protecting autonomy on the exclusive regulation of information. On the contrary, from a methodological point of view, the phenomenon will question the pivotal role of the traditional information approach well established in European consumer law, with specific attention to the mandatory disclosures and the inspired principles. Current rationales will need to be discussed because the protection of autonomy is not only and not anymore, the result of consumer information choice. Put differently, digital consumer autonomy is concerned with the design, development, and implementation of AI systems, as they ensure biases are removed. This observation represents the turning point of this book in comparison to the status quo of existing research.[6]

authorities, to take corrective actions. Sweep results are available at: <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418> accessed 1 September 2023.

[4] Colin M. Gray, Yubo Kou, *et al.*, 'The Dark (Patterns) Side of UX Design' Conference on Human Factors in Computing Systems (2018) CHI Paper 534, 1-14; Jamie Luguri, Lior Jacob Strahilevitz, 'Shining a Light on Dark Patterns' (2021) 13 Journal of Legal Analysis 43-109.

[5] Julian Runge, Daniel Wentzel, Ji Young Huh, *et al.* 'Dark patterns' in online services: a motivating study and agenda for future research' (2023) 34 Mark Lett 155-160.

[6] Principles such as reliability, risk assessment, and human oversight of algorithm-driven systems, which are still crystallized in the EU recent legislative initiatives need to be reviewed. The Academic community has already developed a critical dialogue toward

The lively debate is global. The information approach was (and in many circumstances still is) a pervasive inspired mechanism in EU law and other jurisdictions. Mandatory information obligations responded to different political rationales: in the US, the wide use of mandatory information became the most acceptable solution for contrasting market failure without interfering with deregulation and the free-market principle. On the other hand, in Europe, the strengthening of information duties is in line with the protection of fundamental rights, particularly self-autonomy, and the aim to acquire a high level of consumer protection. Nevertheless, the likewise failure of mandate disclosures has already been emphasized by legal scholarship.[7]

The specific technological change derived from digital design inherent in dark pattern techniques has not gone unnoticed in the European Union (EU).

Based on these observations, the perspective and methodology here adopted will lead to consider the multiple nature of the concerns which arise across different legal fields, including data protection consumer law, with specific attention to unfair commercial practices and competition law, exploring how the distinction between these policies is far from being clear-cut in data-driven consumer markets. Moreover, the nature of the problem will imply considering to what extent data protection law, consumer law and completion law are currently open to embed essentially valuable insights proposed by behavioural economics and other non-legal studies, which become central to understanding what causes the evolution of autonomy in the digital environment (e.g. human-computer interaction). Behavioural consumer data can and should inform the design of private and public choice architectures. 'Choice architects' should steer people toward outcomes that make them better off (according to their interests, not the choice architects) but leave it to the people being nudged to choose for themselves.

At the scope of investigating new suitable regulatory directions for protecting autonomy, it is functional to consider the difference between the shades of meaning inherent in the polyhedric definition of autonomy (e.g. the philosophical, the psychological) and the legally protected

them. See the paper written for the European Law Institute (ELI) by Teresa Rodriguez De Las Heras Ballell, 'Guiding Principles for Automated Decision-Making in the EU' (ELI Innovation paper), European Law Institute, Wien, 2022.

[7] Among other Authors, see Omri Ben-Shahar, Carl E. Schneider, 'The Failure of Mandated Discourse' (2011) 159 U Pa L Rev 647.

perceived autonomy in the fast-moving marketplace automation. Indeed, ethical questions raised by the interaction between automation in smart products and consumer autonomy:[8] to exemplify it is challenging to identify the boundaries of manufacturers' responsibility and liability, given that autonomous products, for example, robotic hoovers, can enable the conditions of personal autonomy, by freeing the individual from undesirable chores or by offering new and hitherto impossible opportunities (such as enabling blind and visually-impaired people to drive a car and thereby enhance freedom of movement). Even the emergence of virtual worlds (e.g. Metaverse or augmented reality) reignites interest in 'first generation' explorations of what consumer autonomy is and what role it should play in today's marketplace.

The forward-looking perspective this book seeks to consider is the relationship between deceptive designs, the new nature of human-digital architecture interaction, and the techno-legal paradigms to protect digital consumer autonomy.

The expected findings will individualize the directions for future changes and enhancements in European private law to build up constructive observations to approach the different EU policies in some measure touched by the problem of dark patterns. From a pragmatical point of view, new legal tools and models will be suggested, mainly belonging to the regulation 'by design' approach. They will be suitable to integrate the protection of autonomy through the regulation of transparency and digital architecture in synergy. Incidentally, the discussion of EU regulatory models will also regard the impact dark pattern tactics have in blurring the line between traditional legal foundations and taxonomies of private law.

Two premises inform this analysis: the awareness of the evolving regulatory environment to meet new user protection exigencies and, consequently, the need to frame the analysis in light of the typical traits of law and technology studies. The acknowledgement that consumers nowadays live an *onlife* dimension,[9] where contemporary digital choice architectures essentially offer an infrastructure to automate the continuous search for exploitable consumer vulnerabilities already constitutes the new

[8] Quentin André, Ziv Carmon, Klaus Wertenbroch *et al,* 'Consumer Choice and Autonomy in the Age of Artificial Intelligence and Big Data' (2018) 5 Cust Need and Solut 28, 37.

[9] Luciano Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* (Cortina Raffaello 2017).

perspective of this study. Business analytics and optimization practices are aimed at finding out how to get consumers to engage with products and services and how to convert them as efficiently as possible.

Necessarily, new legal perspectives must be taken into account at the outset. Firstly, leading scholars have emphasized the importance of legal analysis over a dual regulatory dimension of the digital environment, which inherently combines normative (rule-based) and non-normative (technologically managed) elements when investigating issues concerning law and technology. Increasingly, consumers act in contexts governed by algorithms, meaning new social ordering and decision-making systems regulate a domain of activities and manage risk or alter behaviour through continual computational generation of knowledge by systematically collecting data to attain a pre-specified goal. Consequently, every legal consideration about consumers' autonomy will have to be interconnected with the new challenges belonging to the three stages of the cybernetic process, namely standard setting (adaptive vs fixed behavioural standards), information-gathering and monitoring (historic data vs predictions based on inferred data) and sanction and behavioural change (automatic execution vs recommender systems).

Secondly, legal research in current times needs to correctly map the contours of the emerging insights from other fields of knowledge affecting autonomy in digital consumer choice. In this sense, human-computer interaction, governance studies, surveillance studies, design studies and behavioural economics will contribute to understanding debates surrounding algorithmic regulation, drawing upon these to highlight various concerns about the legitimacy of algorithmic regulation.

Lastly, this study will be profoundly shaped by the fact that the use of Big Data analytics and artificial intelligence 'could recalibrate the relationship between law and individuality and change the foundational structures of our legal systems'.[10] From this perspective, an emerging debate on 'personalized law' takes place. Tailoring legal rules on specific individuals and circumstances will indeed affect the consideration of suitable thresholds of legal protection of the right of autonomy in light of individual consumer characteristics and the effectiveness of legal rules and enforcement.

The book adopts a three-sided structure to explore the topic. The first part (Chapter I) lays the ground by framing the concept of autonomy within current law and technology features, which sets up this research

[10] Christoph Busch, Alberto De Franceschi, *Algorithmic Regulation and Personalized Law* (Hart Publishing 2021) 1.

inquiry. This preliminary part is, in turn, divided into three sub-sections: the first (i) is dedicated to the introduction of the concept of consumer autonomy from a diachronic perspective based on the evolution in EU private law; the second (ii) frames the topic within current regulatory features, functional to analyse in the field of data-driven technologies; and within this last perspective, the third section (iii) offers particular relevance to the renewed importance of the connection between data-driven technological features, autonomy and the traditional information approach, which still represents the basis of current EU consumer protection legislation.

The second part (Chapter II) concentrates on protecting autonomy when dark patterns have tricked consumers. This central part will consider several types of harm caused by dark patterns, including material harm, such as financial harm or anti-competitive issues, as well as non-material harm, such as privacy invasion, time loss, addiction, cognitive burdens, loss of self-determination, and emotional or psychological distress. Through a comprehensive case law analysis, it investigates whether harm caused by dark patterns becomes a constraint for user autonomy. The consumer proved injury could give rise to redress under the consent requirement, or other requirements provided by data protection law, consumer law remedies, or competition law. This analysis will let us understand how people's clicks can be manipulated by dark patterns and to what extent this circumstance is contemplated by current law (e.g. GDPR, DSA, DMA, UCPD), underlining the importance of combining transparency with fairness principles in designing digital architectures. It critically emerged the specific deficiencies of the 'information approach' and the current judicial responsibility test (e.g., fairness test) in achieving, in practice, the protection of the consumer's autonomy, which it was formally designed to achieve.

Finally, based on the previous findings, the third part (Chapter III) reframes the legal inquiry into the effective protection of consumer autonomy under the constrains of dark patterns, suggesting which traditional legal concepts need to be reviewed and which legal model could be more effective and why. Insights gained from behavioural economics and other fields of knowledge can be used as the basis for a more effective and holistic vision of consumer regulatory design in order to respect the principle of consumer autonomy, which still is now a cornerstone principle of EU internal market law.[11]

[11] Annette Nordhausen Scholes, 'Behavioural Economics and the Autonomous Consumer' (2017) 14 Cambridge Yearbook of European Legal Studies 297-324.

I

REFRAMING CONSUMER AUTONOMY INTO THE DIGITAL WORLD: CURRENT MINDSETS

1. Setting the scene

Much has been said, over the years, about consumer autonomy.

Notwithstanding the significant volume of contributions on the subject matter,[1] today it requires recognising the evolution of the concept itself, particularly during two recent stages: firstly, within the predominant online market and considering changes in commercial practices; secondly, taking a step forward, in light of Big Data and artificial intelligence uses.

Indeed, disruptive digital elements impact the traditional concept of autonomy and cause a turning point in European private legal research.

Such elements are various, numerous, and not constantly emerging from a sole legal perspective: they have emerged from the interdisciplinary studies of law, regulation, and technology, which offer a frame for an ambitious set of scholarly inquiries, each one evoking ideas of 'disruption' of legal doctrine and its normative foundations. These studies comprehensively contribute to setting the scene for regulatory frameworks that are 'fit for purpose' in light of rapid technological developments.[2]

In summary, Chapter I is dedicated to reconstructing the concept of autonomy in European Private Law (section 1), starting from the description of functional (section 2 ff) and regulatory (section 3 ff)

[1] Legal Literature relates to the principle of autonomy is extensive. See below note 11 for a reconstruction of the main contributes.

[2] Studies on the crossing area of 'Law, Regulation and Technologies' investigate disruptive technologies. See: Roger Brownsword, Eloise Scotford, Karen Yeung, 'Law, Regulation, and Technology: The Field, Frame, and Focal Questions' in Roger Brownsword, Eloise Scotford, and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford Handbooks-Oxford Academic 2016; 2017 online ed).

disruptive elements that lead to evolution in the way private lawyers will investigate and deal with the polyhedral concept of autonomy.

The usual lenses through which autonomy is considered are rights-based, contractual, and regulatory. Today, the advanced technology-mediated environment requires a deep understanding of online market manipulation and the differentiation between the concrete individual risks and the perceived risks, distinguishing online nudging practices from other more severe forms of nag and manipulation, as well as their practical impact on users and how current law protects the right of autonomy under these circumstances.

In sum, the following pages distinguish disruptive elements based on their nature: the functional nature related to technological aspects and the legal.

From the functional point of view, it is essential to highlight how Big data and AI introduce circumstances into the digital market where digital consumer transactions take place, which are novel compared to previous online market strategies. Suppose potential benefits of Big Data are evident, as the availability of online services for consumers that otherwise would have been paid with traditional currency. In that case, consumers need to be more fully aware of the threats inherent in the commercialisation of personal data. This refers not only to the well-known legal value personal data has acquired with the provision of data as a counter-performance,[3] but also to the exploitation of the consumer preferences inferred by sensitive data and metadata.[4]

Now data-driven technologies can more easily differentiate the information content into unstructured fields than in the past. To achieve this progress, techniques known as web scraping, natural language

[3] See Parliament, Council Directive (EU) 2019/771 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, 28-50.

[4] Metadata are commonly defined as 'data on data' (e.g. the proprieties of a document). Metadata relate to information generated by the communication. They can use to great advantage, as they can reveal latitude, longitude and altitude of the sender's or recipient's terminal, direction of travel, any naming, numbering or addressing information, volume of a communication, network on which the communication originates or terminates, and the beginning, end or duration of a connection. See Nora Ni Loideain, 'EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era' (2015) 3 Media and Communications - Special Issue on Surveillance: Critical Analysis and Current Challenges 53.

processing, and machine learning describes a way of imparting meaning and structure to messy data.[5]

From the legal point of view, it is essential to recognise the effects of planning the regulatory response into the current frame which evolves in turn. These legal changes can also be considered disruptive, and the need to shift the legal reasoning into a *law 3.0* landscape is evident.[6] The European New Deal for Consumers exemplifies a step forward in this direction.[7] Still, it fails to liberate itself from the old paradigms of consumer protection rooted in the pre-Big Data era, as it still seeks to reach its scope by addressing the inequality of bargaining power in consumer transactions.[8] In 2018, the position expressed by the European Commission was to fill the regulatory gaps in consumer law.[9] Early signs of a necessary shift emerged in the legal debate currently developed by legal institutions, indicating the need for a holistic regulatory response reforming the consumer law.[10] Indeed, the growing interplay between consumer law and other different areas of law will demonstrate the complexity of setting a regulatory response into the existing framework.

Consequently, the current Chapter is devoted to emphasising the disruptive elements in cyberspace and pointing out the new legal mindsets and suitable methods to set the research question (section 4) about the

[5] Liane Colonna, 'A Taxonomy and Classification of Data Mining' (2013) 16 Smu Sci & Tech L Rev 309, 332-34.

[6] The expression Law 3.0. was introduced by prof. Roger Brownsword: See Roger Brownsword *Law 3.0. Rules, Regulation, and Technology* (Routledge 2020). The latest developments in technology offer regulators the possibility of employing a technical fix rather than just relying on rule. Thinking like a lawyer might continue to be associated with Law 1.0, but from 2020 onward, Law 3.0 is the conversation that the Author suggested to join. Indeed, the evolution of legal reasoning cannot be adequately understood unless we catch the significance of technology to shaping legal doctrine and our regulatory thinking.

[7] Commission, 'Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee a New Deal for Consumers' COM (2018) 0183 final.

[8] For an interesting analysis of the three intertwined issues of vulnerability, autonomy, and regulation after the New Deal see: Mateusz Grochowski, 'European Consumer Law after the New Deal: A Triptych' (2020) 39(1) Yearbook of European Law 387-422; and Max Planck Private Law Research Paper No. 21/24, available at <https://ssrn.com/abstract=3920452> accessed 1 May 2021. See also Mateja Durovic, Franciszek Lech, 'A Consumer Law Perspective on the Commercialization of Data, European Review of Private Law' (2021) 5 European Review of Private Law 701, 703 and 708.

[9] Commission, Communication (n 7), pages 3-4 of the document.

[10] The observation emerged during the *Second Annual Digital Consumer*, webinar organized by the Commission on 21st November 2022, Brussels.

regulatory response to protect autonomy under the pressure of dark patterns.

1.1 Consumer autonomy in private law: a diachronic perspective

Likewise, the debate in other disciplines emphasises, autonomy is difficult to define in law.[11] A succinct overview of the most traditional conceptual roots will follow.

Over the years, private law scholars have debated the extension of the concept and its constraints, predominantly within the field of contract law.[12] Leading Italian scholarship, for example, considers autonomy as a source of contract, defining it as the parties' ability to self-regulate their interests.[13] The definition is broad,[14] and the

[11] Researchers from different academic quarters, such as philosophy, psychology, and consumer policy have investigated personal autonomy, using different terminologies: while some directly use autonomy, others have relied on different constructs, such as self-determination or free will. See Quentin, Carmon, Wertenbroch, *et al.* (n 8) 28-37; Hans W. Micklitz, 'The principles of European contract law and the protection of the weaker party' (2004) 27(3) J Consumer Policy 339-356; Stephen Vogenauer, Stefan Weatherill, Petra Weingerl, 'Private autonomy and protection of the weaker party' in Stephen Vogenauer, Stefan Weatherill (eds), *General principles of law: European and comparative perspectives* (Studies of the Oxford Institute of European and Comparative Law, Hart Publishing, 2023) 255-268. The topic of consumer autonomy has, for example, a long history in marketing ethics: main representative scholars are Richard H. Thaler and Cass R. Sunstain. See: Richard H. Thaler, Cass R. Sunstain, *Nudge: Improving decisions about health, wealth, and happiness* (Penguin Books 2009); Cass R. Sunstein, 'Fifty shades of manipulation' (2015) 1(3-4) Journal of Marketing Behaviour 214-244. See also Roger Crisp, 'Persuasive advertising, autonomy, and the creation of the desire' (1987) 6(5) Journal of Business Ethics 413-418. For a short description of autonomy in marketing ethics see also Michael R. Hyman, Alena Kostyk, David Trafimow, 'True Consumer Autonomy: a Formalization and Implications' (2023) 183(3) Journal of Business Ethics 841, where the Authors identified the four variables of consumer autonomy: true autonomy, actual autonomy, reliability of wills, and reliability of products choices.

[12] For a reconstruction of the evolution within the Italian civil law field, see Michael W. Monterossi, 'Autonomia del consumatore e morfologia del mercato' (2020) III *Rivista di diritto bancario* 1-35. For a comparative contribute on the principle of autonomy in EU and the Member States see: Peter Christian Müller Graff 'Basic Freedoms: extending Party Autonomy across Borders' in Stefan Grundmann (ed.), *Party Autonomy and the Role of Information in the Internal Market* (de Gruyter 2001) 135-50; and André Janssen, Geraint Howells (eds.), *Information Rights and Obligations: A Challenge for Party Autonomy and Transactional Fairness* (Routledge 2005).

[13] Francesco Gazzoni, *Manuale di diritto privato* (VII ed., ESI 1998) 730. The number of Italian writings and chapters within the handbook of private law dedicated to autonomy is

concrete meaning depends on the interpretative theory of contract lawyers have embraced.[15] Therefore, in principle, party autonomy explicates itself in three ways: the exercise of the freedom to reach, or not to reach, an agreement; the freedom to choose the content of the agreement, with the contracting party; and the freedom to set up a typical, or atypical, contractual agreement.

Among the National jurisdictions, even the European Union has recognised party autonomy as one of the fundamental principles of freedom and market.[16] Europe greatly strengthened the protection of autonomy during the Nineties with the introduction of a specific category of the consumer contracts, the standard contracts.[17] The Court of Justice of the European Union (hereafter: ECJ) has an active role in interpretating key concepts of consumer contracts, leading to harmonisation of consumer law in European legal systems.

Efforts of the ECJ expressed, mainly in 'take it or leave it' situations, through its evolutionary interpretative opera of authentic party autonomy protection regardless the formal respect of legal rules on consent.[18]

extensive. Among others, see: Guido Alpa, 'Autonomia contrattuale' I Encicl. dir.-I tematici (Giuffrè-Francis Lefebvre, Milano, 2021) 1; Alberto Trabucchi, *Istituzioni di diritto civile* (Cedam, 2005) 166; Nicolò Lipari, *Diritto private europeo* (vol 2, Cedam 1997).

[14] See Art. 1322 Italian Civil Code. For a comment: Giorgio Cian, Alberto Trabucchi, *Commentario breve al Codice civile - sub* Art. 1322 (VII ed., Cedam 2005) 1409.

[15] The different theories are summarized by Gazzoni (n 13) 731-734.

[16] EU consumer protection policies are based on Articles 4(2)(f), 12, 114 and 169 of the Treaty on the Functioning of the European Union (TFEU), as well as Article 38 of the Charter of Fundamental Rights of the European Union. Specifically, article 4(2)(f) configures consumer protection as a shared competence between the Union and the Member States.

[17] The milestone has been represented by the Unfair Contract Terms Directive (Directive 93/13/EEC) which protects consumers against unfair standard contract terms imposed by traders (amended by the Parliament Directive (EU) 2019/2161 of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328). For an extensive historical excursus see Gian Antonio Benacchio, 'Diritto privato dell'Unione europea' (Cedam, 2016). See also Gian Antonio Benacchio, 'Pregi e difetti del modello europeo di tutela del consumatore' (2021) 11 Revista Universul Juridic 13-27. The author points out that this legal regime has introduced substantive changes in European private law: it has created a special category of contracts different from general contract law.

[18] On the contrary, well-established scholarship underlined that when consumers «hav[e] a good ability to consume and process information, one will naturally see information as an effective protective tool which enhances the autonomy of the

With the increase of business-to-consumer cases, it is easy to note that traditional rules, such as that of consent, do not always guarantee the freely expressed will of the weaker contracting party. There are endemic conditions in standard contracts that deprive the consumer of that capacity, even when businesses comply with the rules.

Practically speaking, any reduction of choices, constraints, or limitations of consumer options, negatively affect actual autonomy. Surely, price, time, and location of the seller can be considered structural elements of choice. In addition, with the extensive use of standard contracts and asymmetric leverage of power between contracting parties, the major legal challenges to provide effective legal protection tools arise from the distinction between the formal and the actual individual autonomy.

In business-to-consumer e-commerce, the analysis will focus on how technology enables businesses to deeply influence consumer choices.[19] Anticipating the core issue of the following pages: consumers decide in circumstances of an increasingly complex information environment; nevertheless, their ability to exercise their authentic autonomy will decrease not only because of the informational overflow and cognitive strain imposed by the online setting but also by attempts to manipulate their freedom of choices through AI and malicious digital architectural designs.

1.2 Autonomy and the traditional information approach in a nutshell

In EU primary and secondary law, the principle of autonomy is not explicitly defined. In EU law, autonomy is only presupposed by Art. 3(3) TFUE,[20] and it is possible to distinguish almost three critical ways in which the EU ensures autonomy: firstly, through the role of information in allowing consumers to make free choices; secondly, by protecting a

consumer». Geraint Howells, Christian Twigg-Flesner, Thomas Wilhelmsson, *Rethinking EU Consumer Law* (Routledge 2018) 31.

[19] Eliza Mik, 'The erosion of autonomy in online consumer transactions' (2016) 8(1) Law, Innovation and Technology 1-38.

[20] Federico Galli emphasises that 'it has not been necessary for the EU to explicitly define autonomy as a fundamental principle: instead, this principle presupposed itself in the EU's legal rules' (Federico Galli, *Algorithmic Marketing and EU Law on Unfair Commercial Practices* (Springer 2022, 216). In the European legal order, private autonomy is a 'regulated autonomy.' EU private law protects autonomy as a goal to be achieved through other policy objectives, firstly, and notably, the achievement of the Internal Market. This analysis is conducted by Hans-W. Micklitz, Yane Svetiev, Guido Comparato, 'European regulatory private law – the paradigms tested' (2012) 31 Erpl EUI Working Papers Law.

specific vulnerable class of consumers; and thirdly, by protecting unfair terms and practices.

Anyhow, there are provisions on the freedom of contract that imply – for many types of contracts – the freedom to choose the contractual party,[21] to determine the contractual terms and conditions and to conclude or not the contract. Restrictions of parties' rights, of course, exist to balance their position and allow the exercise of autonomy and freedom of contract.

The meaning of autonomy as self-determination represents the freedom of development for personal and interpersonal relations, and the freedom of participation in society.

A relevant contribution to the conceptualisation of consumer autonomy has been offered by the German national experience, particularly keen to emphasise the interconnection between the protection of autonomy and the protection of information.

In general, the German judicial establishment of 'informational self-determination' seems to be the most influential national tradition on the conceptualization of the Charter of Fundamental Rights concerning personal data protection. According to the German Constitutional Court, the right to informational self-determination, based on human dignity and the right to personality, guarantees the power of individuals to determine for themselves the disclosure and use of their data in principle.[22]

For the German Constitutional Court, the right to informational self-determination implies a strict limitation of purposes processing and may be restricted by law in pursuit of general interests. Accordingly, the right is interfered with when personal data is processed beyond the individual's control and such interference may only be permitted under specific conditions.

In sum, pragmatically the protection of individual autonomy has been realised primarily through the information paradigm, where information preserves the consumer's freedom of choice. Consumer EU legislation, like all liberal markets, is based on freedom of choice.

Policymakers have been discussing information asymmetry problems for years, since the 1970s, but it was in the 1990s that information

[21] A distinct debate characterized the pre-formulated standard contract terms: the Unfair Contract Terms Directive (Council Directive 93/13/EC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L. 95/29) protected consumer and contractual autonomy from any interference. See Scholes (n 11) 303.

[22] BundesVerfassungsGericht, 15.12.1983, Volkszählungsurteil, BVerfGE Bd. 65, S. 1.

obligations became a standard part of drafting European consumer protection measures,[23] mostly to restore the contractual balance between consumers and traders.[24]

Information obligations became popular in national and supranational legislatures and gradually tend to expand[25], based on the following statement: disclosure is adequate, widely supported across party lines, and costs almost nothing to implement and enforce since the costs of these activities usually land on third parties.

Mandatory information duties were part of various European consumer protection measures (e.g. Council Directive of 13 June 1990 on package travel, package holidays, and package tours (Package Travel Directive),[26] or Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (Distance Selling Directive).[27]

In the European framework, as well as in the US, mandated disclosures are pivotal regulatory tools of both consumer and data policies:

'for those who believe in the free-market principle, information duties have the advantage of regulating lightly and minimising market interference. […] In contrast, from those who focus on consumer autonomy, mandated disclosure is a well-suited tool for increasing consumer self-determination and promoting consumer empowerment'.[28]

[23] A multitude of other consumer protection measures includes: the Package Travel Directive and the Distance Selling Directive, the Consumer Rights Directive.

[24] Natali Helberger, 'Form Matters: Informing Consumers Effectively' (2013) 71 Amsterdam Law School Research Paper <http://dx.doi.org/10.2139/ssrn.2354988> accessed 13 March 2023; Hanneke Luth, Cseres Katalin, 'The DCFR and Consumer Protection: An Economic Assessment' in Filomena Chirico, Pierre Larouche (eds), *Economic Analysis of the DCFR: The work of the Economic Impact Group within CoPECL* (Otto Schmidt/De Gruyter european law pub 2010) 235-276.

[25] Geneviève Helleringer, Anne-Lise Sibony, 'European Consumer Protection through the Behavioral Lens' (2017) 20(3) Columbia Journal of European Law 607; Annette Nordhausen Scholes, 'Information Requirements' in Geraint Howells, Reiner Schulze (eds.), *Modernizing and Harmonizing Consumer Contract Law* (De Gruyter 2009) 213; Stefan Grundmann, 'La struttura del diritto europeo dei contratti' (2002) 48(3) Rivista di diritto civile 365; Geraint Howells, 'The Potential and limits of Consumer Empowerment by Information' (2005) 32(3) Journal of Law and Society 349.

[26] Council Directive 1990/314/ EEC of 13 June 1990 on package travel, package holidays, and package tours (Package Travel Directive) [1990] OJ L 158/59.

[27] Parliament, Council Directive 97/7/EC of 20 May 1997 on the protection of consumers in respect of distance contracts (Distance Selling Directive) [1997] OJ L 144/19.

[28] Cristoph Busch, 'Implementing Personalized Law: Personalized Disclosures' (2019) 86(2) The University of Chicago law Review 309-331, 310.

1.3 The interconnection between autonomy and information in European law

Over the years, the information approach has always retained its central role. Based on the Community Consumer Policy Strategies (2017-2013), providers' information duties remain the same as those set for the previous strategy, in which the high level of consumer protection and its enforcement also included the realization of «better informed and educated consumers, for example through strengthening the role of the European Consumer Centres».[29]

On 25 November 2020, Parliament adopted a Resolution entitled 'Towards a more sustainable single market for business and consumers', highlighting the importance of the durability and reparability of consumer goods and providing consumers with more rights and information to help them make sustainable choices.[30] The Commission continues to co-finance initiatives to improve the provision of information to consumers, such as the European Consumer Centres Network (ECC-Net), as well as information campaigns in the Member States because, as officially stated better information and improved knowledge of consumer rights could lead to enhanced consumer confidence.[31] The ECC-Network provides information and advice on cross-border shopping and handling consumer complaints. A parallel network, FIN-NET, fulfils the same role for complaints about cross-border financial services. The Commission also conducts consumer information campaigns in the Member States and publishes practical guides for consumers.[32]

Even when encouraging new priorities, such as the current sustainability, as part of the circular economy package, the Commission published on 30 March 2022 a Proposal for a Directive on empowering

[29] Commission, 'Communication to the Council, the European Parliament and the European Economic and Social Committee, EU Consumer Policy Strategy 2007-2013' COM(2007)99 final. Hans W. Micklitz, *The politics of justice in European private law: social justice, access justice, societal justice* (Cambridge University Press 2018).

[30] Relevant research includes Parliament (Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies), 'Sustainable Consumption and Consumer Protection Legislation', Bert Keirsbilck et al. (authors) (2020).

[31] Available at: <https://eur-lex.europa.eu/EN/legal-content/summary/eu-consumer-policy-strategy-2007-2013.html> accessed 27 July 2021.

[32] Your Europe Portal plays an important role in offering access to consumer policy information and in gathering different information sources into one reference information Centre. Access to information has been improved through a single digital gateway (Reg. EU 2018/ 1724).

consumers for the green transition through better protection against unfair practices and providing access to better information. The main objective of the proposal is to help consumers make eco-friendly choices by providing them with the necessary information.[33]

Unfortunately, the requirements of information design, including transparency, have not yet been harmonized. In some areas of consumer law, the Consumer Rights Directive (CRD) included, policymakers operationalize the requirements of information transparency in unhelpful general descriptions, such as mandating traders to use 'clear and comprehensible' language without additional elaboration, attention to context, or examples.[34]

Over the years, the role of information and the central function of consumer autonomy has been both confirmed and implemented in National law and in EU case law.[35] Practically speaking, the legislation assumes that there is often an information deficit disadvantaging the consumer, which can be balanced out by giving the consumer relevant information. This information will enable the consumer to make informed choices.

To be a 'well-informed actor' also represents the main feature that characterized the traditional definition of the average consumer, a term coined by the European legislator with the Unfair Commercial Practices Directive (UCPD).[36]

[33] Commission, 'Proposal for a Directive of the European Parliament and of the Council amending Directives 2005/29/EC and 2011/83/EU as regards empowering consumers for the green transition through better protection against unfair practices and better information' COM/2022/143 final.

[34] Helleringer, Sibony (n 25) 607.

[35] On information duties in EU law see: Sandra Kind, *Die Grenzen des Verbraucherschutzes durch Information – aufgezeigt am Teilzeit-wohnrechtegesetz* (Dunker & Humblot, 1997); Norbert Reich, 'Verbraucherpolitik und Verbraucherschutz im Vertrag von Amsterdam' (1993) 3 Verbraucher und Recht. 5; Von Peter Rott, 'Informationspfl ichten in Fernabsatzverträgen als Paradigma für die Sprachenproblematik im Vertragsrecht' (1999) 98 ZVglRWiss 382-409; Peter Mankowski, 'Fernabsatzrecht: Information über das Widerrufsrecht und Widerrufsbelehrung bei Internetauftritten' (2001) Computer & Recht 767.

[36] Parliament, Council Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') [2005] OJ L 149/22.

This legislative development followed the long-standing ECJ case law on misleading commercial practices, which postulates that average consumers are not easily misled.

Quantity and quality of information are always the focus of debate and attention. As a general principle, information is legally complaint if it is free from deception and not misleading. Notwithstanding, it is not always easy to understand when these conditions are met. As anticipated in section 1.1, the ECJ provided a relevant contribution to this purpose.[37] Starting from the need to eliminate obstacles to the free movement of goods, during the last decades, the ECJ has identified the 'informed consumer standard' about the benchmark of the 'average consumer', meaning reasonably, well-informed, into the relevant market of goods or services.

For the first time, in the case *Gut Springenheide,*[38] the Court of Luxemburg defined the consumer as a reasonably well-informed person, observant, and circumspect. This implies that the 'informed consumer' can autonomously distinguish the characteristics of products and understand the message and content of advertising, with an 'average' ability that needs to be ascertained, case by case, about the situation and the peculiarities of the case.

In recent times, the ECJ argued that the formula of the 'reasonably well informed and reasonably observant and circumspect consumer', established in *Gut Springenheide* needed to be updated. The notion of consumer is a reference threshold for the current analysis as it represents a centrepiece of European consumer protection law. For this reason, and due to the most actual pending interpretative EJC judgment, this book will come back to the issue in Chapter 3, as the empirical case studies of dark patterns considered in Chapter 2 will require a final discussion of the traditional notion of consumer, as well as of vulnerability[39] (see Chapter 3).

[37] Case C-465-98, *Verein gegen Unwesen in Handel und Gewerbe Köln eV v Adolf Darbo AG* EU:C:2000:184 [2000]. See also Case C-210/96 *Gut Springenheide* EU:C:1998 [1998]; Case c-99/01 *Gottfried Linhart e Hans* Biffl [2002] ECR I-9375, paras 31-32; Case C-44/01 *Pippig* [2003] ECR I-03095, para 55; Case C-218/01 *Henkel KGaA* [2004] ECR. I-1725, paras 47, 52, 53 Case C-381/05 *De Landtsheer Emmanuel SA c. Comite´ Interprofessionel du Vin de Champagne, Veuve Clicquot Ponsardin* SA [2007] ECR I-3115, para 23.

[38] Case C-210/96 *Gut Springenheide* EU:C:1998:369 [1998]. With paragraph 31 the Court defined 'the informed consumer standard as the presumed expectations of an average consumer who is reasonably well-informed and reasonably observant'. ibid

[39] The pending interpretative EJC judgment has been referred by the Italian Council of State (Section VI) Order on the 10 October 2022 No. 8650 Consiglio di

More recently, the European legislator highlighted new challenges for consumer law within the digital environment, often with specific reference to information duties and behavioural advertising in the online marketplace, where the intermediatory role of platforms crucially facilitated transactions between suppliers of goods and services, and consumers.[40] Today the availability of information about a product or a service are enormously facilitated using reputational feedback systems, where users can publish and obtain information which the supplier does not furnish.

With the aim of 'modernizing' and strengthen consumer rights within digital economy, the Directive 2019/2161/UE on modernisation and better enforcement, adapted the provisions contained in the UCPD and the Consumers Rights Directive (CRD) to the exigencies of the digital environment, primarily implementing transparency ('modernization directive').[41] Even with the risk of distorting consumer economic behaviour, business are obliged by the Modernization Directive to ensure transparency and truthful practices.[42] The new directive also reviewed the previous maximum harmonisation principle adopted in Directive 2005/29/EC on Unfair Commercial Practices and Directive 2011/83/EU on consumer rights. In the past twenty years a shift characterized the European consumer policy from the minimum towards the maximum harmonization approach. For this reason, the approach of the new directive seems to be slightly different from the standard path.[43] Thus, notwithstanding the valuable purpose of the European Institutions behind

Stato italiano (Sez. VI) 10 October 2022 No. 8650 <https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza?nodeRef=&schema=cds&nrg=202110361&nomeFile=202208650_18.html&subDir=Provvedimenti> accessed 3 January 2023.

[40] Alessandra Quarta, 'Il diritto dei consumatori ai tempi della peer economy. Prestatori di servizi e prosumers' (2017) 2 Europa e diritto privato 667; and Roberta Montinaro, 'Online platforms: new vulnerabilities to be addressed in the European legal framework. Platform to consumer relations' (2020) 2 European Journal of Privacy Law & Technologies 54.

[41] Parliament, Council Directive 2019/2161 of 27 November 2019 amending Council Directive 93/13/EEC and Directive 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of Union consumer protection rules [2019] OJ L 328/7.

[42] Montinaro (n 40).

[43] Mateja Durovic, 'Adaptation of Consumer Law to the Digital Age: Eu Directive 2019/2161 on Modernisation and better Enforcement of Consumer Law' (2020) 68(2) Annals of the Faculty of Law in Belgrade. On the traditional general approach to consumer law see also Lucas Forbes, 'Modernizing Consumer Law in the Fourth Industrial Revolution' (2021) 27 Colum J Eur L 203.

the Modernization Directive amendments made to the EU acquis in 2019, they have yet to settle the debate on the risks faced by consumers in the digital age. For legal scholars, this was due to the fact that structural asymmetries related to the rise of online platforms and the increasing sophistication of algorithms deployed by them cannot be solved through isolated amendments alone but require a more in-depth rethinking of the existing framework.[44]

In summary, with the most recent actions of the European Commission for the revision of EU consumer law announced in the New Consumer Agenda 2020 and the Circular Economy Action Plan,[45] information requirements and transparency remain the pillars of the policy in order to empower consumers for green transition, and towards sustainable consumption: the scope of consumer protection will be slightly different, orientated to ensure consumer environment-friendly choices when buying their products, but the legal approach remains the traditional one. Thus, consumer law will be interpreted considering private law rules, which are defined as 'porous' in nature.[46] Hence, always in the perspective of renovating consumer law, the interaction between private law and consumer rules is plausible to protect the interests of individuals throughout the market experience.[47]

1.4 The dynamic concept of autonomy in the digital context...

Thus far, the analysis has shown to what extent, during the last decades, the EU legislator went beyond the vision of autonomy in contract law and company law, exclusively intended as consumers' contractual freedom.[48] Legislators needed to embrace the informational autonomy, especially manifested through the consumers' management of personal and non-

[44] Agnieszka Jabłonowska, Hans-W. Micklitz, 'EU Consumer Law in 2020' (2021), available at <https://ssrn.com/abstract=3843175> accessed 23 June 2023.

[45] Commission, 'New Consumer Agenda Strengthening consumer resilience for sustainable recovery (Communication)' COM/2020/696 final.

[46] Helleringer, Sibony (n 25).

[47] In these terms, see also Antonio Davola, 'Fostering Consumer Protection in the Granular Market: The Role of Rules on Consent, Misrepresentation and Fraud in Regulating Personalized Practices' (2021) Technology and Regulation 76-86 <https://doi.org/10.26116/techreg.2021.007> accessed 13 January 2023.

[48] For the different meanings of contractual autonomy in Member States, see Hans-W. Micklitz, 'On the intellectual history of freedom of contract and regulation' (2015) 4(1) Penn St J Law Int Aff.

personal data, and the freedom to express themselves into the digital environment without being co-opted (personal freedom and fundamental right). This shifting meaning went hand in hand with the goal of the European Union consumer policy to ensure data-subject empowerment: the latter concept was developed to struggle with forms of advertising which invade consumers' freedom.[49] Protecting consumers' genuine preferences through empowerment has become transversal in consumer law and data protection law, with consent possibly being the most evident example to elucidate the interplay with transparency. To sum up, empowerment must entail (i) human agency (a sort of free will), (ii) a sufficient degree of transparency, and (iii) the absence of manipulation.[50]

Digital environment calls for the consideration of a more comprehensive meaning of autonomy. Up to now, few pioneering legal studies have discussed the topic considering the regulation of behaviour modification through the design of choice architectures[51]. Digital context implies the need to enlarge the overview of the elements impacting on autonomy to the extent that some authors have also proposed the adoption of the more comprehensive concept of 'data autonomy', meaning the ability of individuals to have control over their data.[52]

In an over-informed society, everything is performed by algorithm-driven systems. Automation is critical to managing complexity, performing mass activities at an affordable cost, and ensuring effectiveness in processing data, information, and digital content. The way data storage, use, and control are evolving affects the traditional information approach, at the basis of the EU consumer law.[53]

[49] Council Resolution of 14 April 1975 on a preliminary programme of the European Economic Community for a consumer protection and information policy and Preliminary programme of the European Economic Community for a consumer protection and information policy, 25 April 1975, O.J. C 92. On the topic of empowerment, see in particular: Jan Trzaskowski, *Your Privacy Is Important to Us! – restoring human dignity indata-driven marketing* (chapters 6 and 7, Ex Tuto 2021).

[50] ibid

[51] Jan Trzaskowski, 'Persuasion, Manipulation, Choice Architecture and 'Dark Patterns' in Jan Trzaskowski (ed.), *Your Privacy Is Important to Us! – restoring human dignity in data-driven marketing* (Ex Tuto 2021), available at <www.ypii.eu> accessed 13 May 2023. See also Andrej Savin, Jan Trzaskowski (eds.), *Research Handbook on EU Internet Law* (2nd edition, Edward Elgar 2023).

[52] Cesare Fracassi, William Magnuson, 'Data Autonomy' (2021) 74 Vand L Rev 327.

[53] Scholes (n 11) 297; Gerd Gigerenzer, *Decisioni intuitive. Quando si sceglie senza pensarci troppo* (Raffaello Cortina editore 2009). Gigerenzer explains why many decisions are not rational but based on mere intuition: they can be based on heuristics (shortcuts in

Today, the advanced technology-mediated environment requires taking into account not only the complex information overflow but also the way digital architecture design can manipulate human abilities to make decisions.

The phenomenon of dark patterns, described in Chapter II, as well as other contemporary phenomena, such as personalization and recommender systems and behavioural advertising, showed that new EU regulation introduces novel provisions to respond to the new challenges posed to autonomy but fails to consider long term consequences on autonomy.[54]

Apart from this observation, what counts here is the need to consider the new polyhedral meaning of autonomy in the context of the AI market and data-driven technologies. It is, in fact, essential to recognize the renovated applicable regulatory framework and the consequent enlargement of new remedies against data-driven technologies generating harms to consumer autonomy, which will come from EU data protection law and marketing law.[55]

Considering when the instrumental use of AI technology influences user behavioural tendencies, autonomy will be affected not only by the quantity and quality of data but also by the architectural design.[56] Surely, the design of user interfaces is not a neutral operation. Consequently, it requires these considerations to be part of the new path towards the protection of consumer autonomy which necessarily becomes a dynamic techno-legal analysis.

reasoning), also called 'rules of the thumb'. Having more information available or time to decide, does not lead to better decisions. Simplicity is a form of adaptation to uncertainty.

[54] The Author shares the considerations expressed by Sébastien Fassiaux, 'Preserving Consumer Autonomy through European Union Regulation of Artificial Intelligence: a Long-term Approach' (2023) European Journal of Risk Regulation 1-23, 8. Also consider Thomas Anker, 'Autonomy as License to Operate: Establishing the Internal and External Conditions of Informed Choice in Marketing' (2020) 20(4) Marketing Theory 528; Quentin, Carmon, Wertenbroch, *et al.* (n 8).

[55] Fassiaux, ibid. The Author analyses consumer autonomy through a four-layer prism of principles, which allows to the study the dynamic of autonomy protection: choice, privacy, independency, and reciprocity. He advises EU policymakers to integrate long-term thinking into consumer and data protection regulations because it might become a constitutional requirement if intergenerational solidarity is incorporated into the Treaties, as suggested by the Commission President in 2022.

[56] Statistical data are reported by the consumers' attitudes towards cross-border trade and consumer protection reports, available at <https://commission.europa.eu/strategy-and-policy/policies/consumers/consumer-protection-policy/evidence-based-consumer-policy/consumer-scoreboards_en>.

1.5 … with specific attention to data-driving technologies and (in future perspective) Metaverse

The effects of digitalization on consumer choices have changed with the advent of data-driven technologies and the extensive use of digital data. Disruptive is, in fact, the way they impact on the essential elements of choices, such as the selection of possible options (section 2).

Digitalization is 'one of the ground-breaking trends of this century'.[57] In particular, the phenomenon of the so-called datafication leads to an incredibly fast and increasing mass of data for business processes, transforming economy and social relations. Current peculiarities of the technological environment will mismatch traditional business models, impacting on EU consumer law, data protection law, and other areas of private law (section 3.2).

It has been recognized that data may affect the legal dynamics of the specific object of regulation; the source of law, and the functioning of legal patterns (not formally included in an actual law).[58]

The European data strategy gives a primary role to human beings in developing technology and defending European values and rights in the digital world.[59] It aims at creating a single market for data that will ensure Europe's global competitiveness and data sovereignty, trusting among actors who share data in order to protect fundamental rights and property rights. Common European data spaces will guarantee that more data becomes available in the economy and society while empowering the control of companies and individuals who generate the data.

Data driven applications will benefit citizens and businesses in many ways (e.g. improving health care, generating new products and services, etc). The Commission has proposed a Regulation on European Data

[57] With the mentioned words, the organizers of the Münster Colloquia on EU Law and the Digital Economy (III) of the 2017 introduced a prolific discussion about how digitalization has been transformed the entire economy and society. To read the findings of the Colloquia, see Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools (Münster Colloquia on EU Law and the Digital Economy (III)* (Nomos, Hart Publishing 2017) 13.

[58] Mariavittoria Catanzariti, Deidre Curtin, 'Data at the Boundaries of (European) Law: a first cut', in Deidre Curtin, Mariavittoria Catanzariti (eds.), *Data at the Boundaries of European Law* (Oxford University Press 2023) 6.

[59] Commission, 'A European Strategy for data' (Communication), COM/2020/66/final.

Governance (Data Governance Act) as part of its data strategy (2020).[60] This new Regulation will play a vital role in allocating the EU's leadership in the global data economy. Subsequently, on 23 February 2022, the Commission proposed a new Regulation on harmonized rules on fair access and use of data (Data Act).[61] The Data Act is a critical pillar of the European strategy for data. Its main objective is to make Europe a leader in the data economy by harnessing the potential of the ever-increasing volume of industrial data.

All the significant impacts of data-driven technologies and changes interested the data subject. For example, in the data economy, the way consumers act, participate, and contribute to the sharing economy identifies the so-called 'prosumer' as a new model of consumer. This model is named with a specific expression that combines the words producer and consumer. The expression is not new. The original idea of the prosumer came from a futurist and business writer, who at the beginning of the eighties, reflected the consumer's new proactive role.[62]

With the advent of the so-called Web 2.0 era, also described as the participatory web, the consumer began to self-generate e-content, propose services as well as traditional providers, and share goods.[63] The advent of social media and self-publishing platforms (Wikis, blogs) allowed easier content production and participation by users.

The idea nowadays perfectly matches the consumer (*rectius* prosumer) role, especially in transactions and activities taking place on platforms. The new model impacts on the traditional taxonomy of private law, protecting both parties. Indeed, traditionally, the need to protect the weaker party is one of the principal reasons for limiting bargaining autonomy, mainly because of the inability of either party to enter into agreements on an equal footing with its counterpart. With the emergence of the platform economy, it is widely believed that this need for protection has been

[60] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)', COM(2020) 767 final.

[61] Parliament, Council, 'Proposal for a Regulation on Harmonized rules on fair access to and use of data' (Data Act), COM(2022) 68 final.

[62] Alvin Toffler, *The Third Wave* (William Morrow & Company Inc. 1980).

[63] Parliament, Council, 'Regulation (EU) 2022/1925 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*) [2022] OJ L 265; and the Parliament, Council, 'Regulation Eu 2022/2065 of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (*Digital Services Act*)' [2022] OJ L 277.

drastically reduced.[64] A supportive argument it has to consider the role of the prosumer who, very often, offers a service while possessing similar power and availability of information to the recipient of the service.

Before the European Parliament and the Council agreed on a comprehensive package of legislation establishing new rules for online platforms (the Digital Markets Act and the Digital Services Act of the 2022),[65] scholars advised that the platform itself can control and process a great amount of data with the potential risk of market manipulation.[66] There are precise positions stating how a lack of transparency about the role and status of the parties active in the online marketplace characterised the complex digital environment shaped by platforms. Nonetheless, practices in online platforms are aimed at conditioning consumer behaviour, limiting their self-determination.[67] The ability to differentiate the price, which refers to price discrimination, is an example. Risks of discrimination constrain the possibility for the parties to establish the price themselves and freely decide the price (see section 3.3). Under personalized pricing, businesses segment customers into small groups or individuals, charging each a share of an estimated value of their willingness-to-pay.[68]

[64] The issue is analysed by Guido Smorto, 'La tutela del contraente debole nella platform economy dopo il Regolamento UE 2019/1150 e la Direttiva UE 2019/2161 (c.d. Omnibus)', in Valeria Falce (ed.), *Fairness e innovazione nel mercato digitale* (Giappichelli 2020) 1-22 <https://www.uerinnovationchair.org/wp-content/uploads/2020/06/04-Smorto-049-070.pdf> accessed 18 December 2022. The Author underlined that the new 'peer-to-peer' economy does not always involve equal bargaining power.

[65] Parliament, Council Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1; Parliament and Council Regulation (EU) 2022/1925of 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) [2022] OJ L 265/1. The Digital Services Act and Digital Markets Act set a high global benchmark for regulating digital services with clear obligations tailored to the importance of online platforms.

[66] Yocai Benkler, 'Degrees of Freedom, Dimensions of Powers' (2016) 145(1) Dædalus, the Journal of the American Academy of Arts & Sciences 18; Vasilis Kostakis, Michel Bauwens (eds.), *Network Society and Future Scenarios for a Collaborative Economy* (Springer 2014).

[67] Montinaro (n 40).

[68] See OECD, 'Personalized Pricing in the Digital Era' (Background Note by the Secretariat), 28 November 2018, <https://one.oecd.org/document/DAF/COMP(2018)13/en/pdf>. For personalized price to occur, three fundamental conditions must be satisfied: (1) businesses must be able to measure consumers' willingness-to-pay; (ii) businesses must create a mechanism to prevent

Lastly, even if it is still experimental, Metaverse is emerging as the next disruptive technology in the coming decades by enabling immersive experience through the convergence of the physical and the digital universes. This is true also for augmented reality.[69] Metaverse is expected to revolutionize many fields (e.g. travels, tourism, marketing), as well as shape the future of the consumer research agenda. European Authorities have started to explore the policy issues concerning the advent of Metaverse, in various areas, including competition, data protection, liabilities, and inclusiveness.[70]

2. 'Disruptive' digital architectural design. New room for «legal protection by design»?

Lawyers need to reconsider the traditional approaches towards autonomy to analyse a Web 2.0 scenario and a coming Web 3.0 scenario, also known as the semantic web or intelligent web. Web 3.0 is an 'umbrella term' to describe the third generation of Internet services with its data-driven configuration, powered by the cognitive services of artificial intelligence. Data will be interconnected in a decentralized way, which would be a giant leap forward from the current generation of the internet (Web 2.0), where data is mostly stored in centralized repositories.

In Web 2.0, and with greater extension in Web 3.0, the distinction between professional, semi-professional and consumer will blur: users and machines will be able to interact with the data, and in future perspective through an avatar into the Metaverse. For this to happen, programs must understand the information conceptually and contextually. This is why the

arbitrage; and (iii) businesses must have some element of market power. More documents relating to this discussion can be found at <http://www.oecd.org/daf/competition/personalised-pricing-in-the-digital-era.htm>.

[69] An illustrative example is the mobile game Pokémon Go, which allows the user to interact with virtual creatures, Pokémon (pocket monsters), which appear in the user's real environment identified by GPS signals. As catching Pokémons requires users to be at particular geographic locations, it has been used to drive real visitors to actual McDonald's restaurants and other sponsors. See Josh Constine, 'Pokémon GO reveals sponsors like McDonald's pay it up to $0.50 per visitor' (2017) TechCrunch.

[70] Parliament, 'Metaverse Opportunities, risks and policy implications' (2022) June <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733557> accessed 5 September 2023; Council of the EU, 'Analysis and research team, Metaverse – virtual world, real challenges' (2022) March 2022 <https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf> accessed 3 March 2023.

two cornerstones of Web 3.0 are semantic web and artificial intelligence (AI).

In Metaverse, interoperability will be a crucial feature in legal matters. The multitude of entities in the Metaverse will create a 'web of relationships', blurring roles and making it difficult to determine and allocate responsibilities and liabilities. A new digital architecture that leads to the evolution of users' behaviours and consumers' habits.

It is preliminarily essential to recognize the peculiar nature of the mutual relationship between law and technology[71]: technology as law, and technology as the object of legal regulation; technology as a subject regulating human behaviour. The last one includes the default technological setting that determine the 'choice architecture'.

Along this line of reasoning, digital design, even with the shape of dark patterns, will transform the legal environment and the substance of legal certainty and fairness. Thus, digital design could offer a new or renovate tool for the legal protection of consumer autonomy.

A step back could be helpful. In social sciences fields, such as behavioural economics, findings already demonstrated that informed decisions also relate to the selection of information,[72] which depends not only on rational principles but also on what consumers feel, see or expect to see. Consequently, using behavioural economics findings about consumers' habits or tendencies enable the construction of informational content to nudge consumers. Albeit the concept of nudging will be examined more in-depth in the following paragraph (section 2.1), it can already be noted that this approach can be used with fair intention, improving the consumer position, or with malicious goals, which deserve to be further explored (see Chapter II).

[71] See, among others: Giorgio Resta, 'Governare l'innovazione tecnologica: decisioni algoritimiche, diritti digitali e principio di uguaglianza' (2019) 50(2) Politica del diritto 218; Stefano Troiano, 'Prefazione', in Stefano Troiano (ed), *Diritto privato e nuove tecnologie. Riflessioni incrociate tra esperienze giuridiche a confronto* (ESI 2022) IX; Mirelle Hildebrand, 'Legality by design' or 'Legal protection by design'? (2020) Law for Computer Scientists and Other Folk, <https://doi.org/10.1093/oso/9780198860877.003.0010> accessed 3 May 2023; Matthias Lehmann, 'From Codification to Coding and Digitised Codification: Legal Tech, RegTech, and their Role for the Future of European Private Law' in André Janssen, Matthias Lehmann, Reiner Schulze (eds.), *The Future of European Private Law* (Nomos 2023) 225.

[72] For an example, see the analysis related to traditional food choices: it shows that consumers do not base their choices on information labels: see Cass R. Sunstein, 'Report on Mandatory Labelling, with Special Reference to Genetically Modified Foods' (2016) 165(5) University of Pennsylvania Law Review 1043.

When reasoning about online nudging through web design and architecture, interdisciplinary insights are valuable to lawyers. For example, the multidisciplinary field of studies of human-computer interaction (HCI) has to be taken into account because it helps to understand people and their practices for the design of technology with the ultimate goal of providing a particular perspective in addressing many of the critical issues currently encountered by computer sciences, such as awareness, privacy, context, experience, emotion, and participation.[73] The important contribution of studies is increased by the actual role of the collection, storing and use of information about the customer required by most e-commerce applications in order to offer personalized products and services.[74]

In practice, personalising of advertising and targeting techniques in platforms would introduce new vulnerabilities.

Personalization is about selecting or filtering information objects or products by using information about the user account (e.g. the customer profile), practically meaning the information displayed on the screen is specifically tailored according to the information already available about the user. From a technical point of view, meta-data about products is matched against user information stored in the customer profile (a person group or to a specific individual). There are various ways e-shop operators can cultivate customer profiles: 'implicitly' by storing interaction with the website (click stream) and purchase transactions, or 'explicitly' by asking for preferences and ratings. Scenarios like these are commonly used, and induced legal scholarship to think about the specific changes they can provoke in law. Given the importance these changes represent for the analysis of autonomy, they will be further discussed in section 3.2.

In the online context, many authors have criticized disclosure as inadequate when it comes to engaging and educating consumers in order

[73] Human-computer interaction (HCI) is a multidisciplinary field of study on digital architecture focused on the interaction between humans (the users) and computers. While initially concerned with computers, HCI has now expanded to cover almost all forms of information technology design. HCI aims to design accessible, usable, efficient, and safe systems for everyone. See Benjamin R. Cowan, Leigh Clark, *et al.*, 'Introduction to this special issue. Guiding the conversation: new theory and design perspectives for conversational user interfaces' (2023) 38(3) Human-Computer interaction 159.

[74] See Omri Ben-Shahar, Ariel Porat, *Personalized Law: Different rules for different people* (Oxford University Press 2021).

to correct market imbalances.[75] Some even view contemporary online disclosures as mere compliance instruments that safeguard companies from possible legal action and, thus, were never seriously meant to educate consumers.[76] Yet other scholars are ready to abandon information obligations altogether and instead propose consumer protection measures whose success does not hinge on customer knowledge at all.[77] The role of the design of digital architecture can undoubtedly be pivotal to this aim. Designers become the architects of choices able to benefit from the important contributions from studies on cognitive biases and individual consumer variations when it comes to reading disclosures:[78] they will raise the question whether standardization can ever work. In general, a shift from remedying market failures for defective information obligations to more preventive action (*ex ante* policy) is advocated (see Ch. III).

Critique progresses are also evident. For instance, the European Commission's Consumers, Health, Agriculture and Food Executive Agency (CHAFEA) sponsored a study on consumer attitudes towards contract terms and conditions online.[79] It came on the heels of other consumer research initiatives, most of which fall under the umbrella of behavioural economics and focus on the impact of offline and online

[75] Ian Ayres, Alan Schwartz, 'The No Reading Problem in Consumer Contract Law' (2014) 66(3) Stanford Law Review 545; Yannis Bakos, Florencia Marotta-Wurgler, David R. Trossen, 'Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts' (2014) 43(1) The Journal of Legal Studies; Oren Bar-Gill, Kevin E. Davis, '(Mis)perception of law in Consumer Market' (2017) 19(2) American Law and Economics Review 245; Geraint Howells, 'The Potential and Limits of Consumer Empowerment' (2005) 32(3) Journal of Law and Society 349; Florentia Marotta-Wurgler, 'Does Contract Disclosuce Matter?' (2012) 168(1) Journal of Institutional and Theoretical Economics JITE, 94; Omri Ben-Shahar and Carl E. Schneider, 'The Failure of Mandated Disclosure' (2011) 159 U Pa L Rev 647; Omri Ben-Shahar, Carl Schneider, *More than You Wanted to Know. The Failure of mandated Disclosure* (Princeton University Press 2014).

[76] Steve Furnell, R. von Solms, Andy Phippen, 'Preventative Actions for Enhancing Online Protection and Privacy' (2011) 4(2) International Journal of Information Technologies and Systems Approach 1-11.

[77] See, for example, Lauren Willis, 'Against financial literacy education' (2008) 94 Iowa Law Review paper No. 08-10.

[78] Marianne Bertrand, Adair Morse, 'Information Disclosure, Cognitive Biases, and Payday Borrowing' (2011) 66(6) The Journal of Finance 1865.

[79] Maartje Elshout, Millie Elsen, Jorna Leenheer, *et al.*, 'Study on Consumers' Attitudes Towards Terms Conditions (T&Cs) Final Report for the European Commission, Consumers, Health, Agriculture and Food Executive Agency (Chafea) on behalf of Directorate-General for Justice and Consumers (September 22, 2016) <https://ssrn.com/abstract=2847546>.

information on consumer choices in healthcare,[80] and sustainability-related behaviours.[81]

2.1 Different digital designs to nudge…

Computer language and new digital designs introduce a wide range of tools, as well as critical issues, in the set-up of the human-centred interaction between the user and the digital world.[82] Today, HCI goes much further, also covering the process of designing and prototyping legal artefacts, services, organizations, and systems.

Persuasive techniques are also well explored by behavioural economics, while their effects on law, specifically on consumer autonomy, are a much more recent object of study. For this reason, it is opportune to start with a recognition of the contribution of behavioural economics to grasp the biggest changes of perspective a lawyer needs to acquire in assessing technological risks.

A helpful starting point is the distinction between nudging and manipulation because persuasive nudging can also be easily transformed into manipulation: the distinctive line is thin.

Thaler and Sunstein define a nudge as follows:

'any aspect of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not'.[83]

[80] Alberto Alemanno, Anne-lise Sibony (eds), *Nudge and the Law: A European Perspective* (Hart Pub. 2015).

[81] Stefanie Lena Heinzle, Rolf Wustenhagen, 'Dynamic Adjustment of Eco-labelling Schemes and Consumer Choice – the Revision of the EU Energy Label as a Missed Opportunity?' (2012) 21(1) Business Strategy and the Environment 60-70.

[82] HCI is the subject of technology ethics studies, which has isignificant connections with other related fields of study, such as Science and Technology Studies (STS), Privacy, Ethics and Law. See Colin M. Gray, Cristiana Santos, Natalia Bielova, Michael Toth, Damian Clifford, 'Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective' (2021) CHI Conference on Human Factors in Computing Systems (May 8-13 ACM, New York, USA) <https://doi.org/10.1145/3411764.3445779> accessed 10 May 2023.

[83] Richard H. Thaler, Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Revised and Expanded Edition, Penguin Books 2009) 6.

With those words, the Nobel Prize economists introduced the theory of nudging, which had become a popular approach for designing new regulatory strategies and public policies based on the opposite rationale rather than the traditional command-and-control one: persuasion.

Persuasive knowledge refers to the capacity of consumers to understand that there is an attempt to persuade them and for them to activate defensive reactions.[84] The level of awareness about a persuasive attempt and the capacity to exert a critical screening against it needs to be measured. However, this theory, developed for traditional media, fails to account for the interactive nature of consumer online experience and for how such interaction can subvert the persuasion knowledge and related awareness a consumer might have.[85] Awareness requires attention. However, attention is limited,[86] as are all cognitive resources available to consumers to process information and execute decisions.

Online interaction absorbs some of these resources, leaving consumers more exposed and less vigilant. Problems can arise if persuasion activates an emotional load guiding consumer choice (affect heuristic),[87] or induces a misperception of risks (probability neglect).[88] This could also depend on the levers of influence, identified in Cialdini's thought-provoking book with seven levers, namely: reciprocation, liking, social proof, authority, scarcity, commitment and consistency, and unity.[89]

Thus, even if persuasion knowledge could be activated initially, effort (cognition) and enjoyment (affect) may neutralize the recognition of the persuasive intent of an offering, where the message is processed below the level of conscious awareness. This is further compounded if the

[84] 'Persuasion Knowledge Model' or PKM: Marian Friestad, Peter Wright, The Persuasion Knowledge Model: How People Cope with Persuasion Attempts (1994) 21(1) Journal of Consumer Research 1-31.

[85] Applying Kahneman's limited capacity of attention model (Amos Tversky, Daniel Kahneman, 'Availability: a heuristic for judging frequency and probability' (1973) 5(2) Cognitive Psychology), it is possible to formulate a rival hypothesis to that of persuasion knowledge, a hypothesis in line with the concept of 'attention deficit'.

[86] ibid

[87] Paul Slovic, Ellen Peters, 'Risk Perception and Affect' (2006) 15(6) Current Directions in Psychological Science 322.

[88] Cass R. Sunstein, *Republic.com. Cittadini informati o consumatori di informazioni?* (il Mulino 2003).

[89] Robert B. Cialdini, *Influence, New and Expanded* (Harper Business 2021, first published 1984).

consumer is characterized by permanent (i.e., age, mental infirmity, etc.) or transient (psychological state at any given moment) forms of vulnerability. In other terms, some scholars described with the term 'friction' the effect of persuasive technology, which relies on the preference for cognitive ease, practically creating a sort of perceiving obstacle to instant gratification.[90]

The online interaction, depending on the nature of the design interfaces, can lead consumers to enter a state of flow whereby, when an experience is genuinely satisfying, individuals are so absorbed and focused that their persuasion knowledge is neutralized. Finally, social cognitive theory suggests that peer pressure mechanisms may also offset persuasion knowledge.[91]

The tendency to influence policymakers with insights proposed by cognitive psychologists and behavioural economists through the nudge theory has become widespread during the past few decades, to the extent that the utility of nudges was also recognized at the international level by the Organization for Economic Co-operation and Development (OECD) as a trend impacting on several policy domains, including the consumer policy.[92]

The nudging theory is, indeed, a form of techno-social engineering.[93] It starts from the consideration that human beings act irrationally (contrary to the views of classical economists) and, consequently, that people often make costly mistakes.[94] Therefore, consumers need incentives and help to make decisions that are in their best interest.[95]

The idea behind nudging is libertarian paternalism: paternalism because there is a clear indication of the path, libertarian because there is no obligation to follow it. This guiding principle is flexible and can be adapted to all levels and policies. It can be used in all kinds of institutions, public or

[90] Brian J. Fogg, *Persuasive Technology* (Kaufmann 2003).

[91] Albert Bandura, 'Social Cognitive Theory: An Agentic Perspective' (2001) 52 Annual Review Psychology 1-26.

[92] OECD (Directorate for science, technology and innovation committee on consumer policy), 'Use of Behavioral in Consumer Policy' (2016) Nov. 7-8, 4.

[93] Brett Frischmann, Evan Selinger, *Re-Engineering Humanity* (Cambridge University Press, 2018).

[94] Herbet A. Simon, *Model of bounded rationality* (MIT Press 1982).

[95] A dual model of decision-making was described: 'System 2 nudges' are aimed at people's slow cognitive thinking and deliberative decision-making, whereas 'System 1 nudges' target people's rapid, intuitive decision-making mode. The mind functioning was described by Daniel Kahneman, *Thinking, fast and slow* (Farrar Strauss& Giroux 2011).

private if policymakers and the system of rules conform to the desire of those who designed the model.

In essence, nudges can shape the setting for the choice architecture. Friction, for example, in all its forms (e.g. reading, clicking, scrolling, paying) plays a key role when it is part of the design of online experiences. A clear example is the context of cookie consent pop-ups. Nudges can be positively altered by driving real and lasting behavioural changes. Depending on the implementation of rules about infrastructure, different responses from the recipients will arise.

The policies on vaccines represent another example, as empirical studies demonstrate how getting a vaccination implies a decision under conditions of uncertainty that leads to the overestimation of some risks (the adverse effects of vaccines) and underestimation of others (the danger of getting sick).[96] Legal scholarship investigates the most valuable tools to encourage vaccination practice: the COVID-19 pandemic increases the urgency of undertaking nudging-focused research, to understand, for example, if it would be a concrete incentive to grant permission to enter to cinemas only to citizens possessing the 'green-pass'.[97]

Behavioural data is the fuel of the design architecture. The implied logic of the nudge theory is data-driven social engineering data. Consequently, there are no neutral designs for architects,[98] meaning that they should be aware of the mechanisms that govern human choices. Individual decisions are, in fact, often driven by heuristic-based reasoning, as opposed to the pure optimization approach presumed by rational choice theory.[99]

In sum, heuristics are devoted to simplifying complex decisions. Through them, an individual substitutes a problematic question with an easier one, as heuristics are a sort of generalization that helps individuals to

[96] Daniel M. Kahan, 'Vaccine Risk Perceptions and ad hoc Risk Communication. An Empirical Assessment' (2014) 17 Ccp (Risk Perception Studies Report) Yale Law & Economics Research Paper No. 491.

[97] Shusaku Sasaki, Tomoya Saito, Fumio Ohtake, 'Nudges for COVID-19 voluntary vaccination: How to explain peer information?' (2022) 292 Social Science and Medicine 114561.

[98] Thaler, Sunstein (n 83).

[99] For a long time, economic policy has been based on the *homo oeconomicus*, a neoclassical model of a rational subject always able to find out information about the best product option, balancing cost, benefits and his own preferences. Herbert Simon introduced the term 'bounded rationality', as a shorthand against the neoclassical economics model: he suggested replacing the perfect rationality assumptions of *homo economicus* with a conception of rationality tailored to cognitively limited agents. See Herbet A. Simon, *Model of bounded rationality* (MIT Press 1982).

judge immediately but often result in irrational or inaccurate conclusions. They act as cognitive shortcuts under conditions of uncertainty.

In this field, a crucial contribution was made around the early 1970s by a series of papers written by Amos Tversky and Daniel Kahneman that revolutionized academic research on human judgment[100]. Daniel Kahneman also received the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel on 2002 for integrating insights from psychological research into economic sciences, especially concerning human judgment and decision-making under uncertainty.

Based on Kahneman's findings, uncertainty is an unavoidable condition: individual choices must be taken:

'on beliefs about the likelihood of such uncertain events as the guilt of a defendant, the result of an election, the future value of the dollar, the outcome of a medical operation, or a friend is response. Because we normally do not have adequate formal models for computing the probabilities of such events, intuitive judgment is often the only practical method for assessing uncertainty'.[101]

Over time, the number of heuristics, and biases identified in psychology have enormously increased from the original ones: availability, representativeness, anchoring and adjustment.[102] Likewise, the application of the theory spread into many different disciplines, including economics, law, medicine, and political science.

[100] Writings were collected in a very influential book by Amos Tversky, Daniel Kahneman, 'Judgment under Uncertainty. Heuristics and Biases' (1974) 185(4157) «Science» New Series 1124-1131; Daniel Kahneman, Paul Tversky, Amos Slovic, *Judgment under Uncertainty. Heuristics and Biases* (Cambridge University Press 1982). For an overview see Thomas Gilovich, Dale Griffin, Daniel Kahneman (eds.), *Heuristics and Biases: The Psychology of Intuitive Judgment* (Cambridge University Press 2002).

[101] Amos Tversky, Daniel Kahneman, 'Extensional versus Intuitive Reasoning: The Conjunction Fallacy in Probability Judgment', in Gilovich, Griffin, Kahneman (eds.), ibid, 19-48.

[102] The 'Rules of thumbs' expression was coined in 1973 by Amos Tversky and Daniel Kahneman. In short, for the Authors: the heuristic of availability unconsciously occurs and operates under the following principle: 'if you can think of it, it must be important'. Thus, things that come to mind more easily are believed to be far more common and more accurate reflections of the real world; the representativeness heuristics facilitate answers to questions related to the probability of the realization of random events, the future development of variables or the probability that a specific object belongs to a certain group; the anchoring effect is a tendency for a person to rely heavily on the first piece of information they receive when making decisions. See A. Tversky, D. Kahneman (n 85), 1124-1131.

Consumer behaviour and consumer policy are exemplary contexts for behavioural economics to contribute:[103] it was demonstrated that consumer decisions are subjected to systematic bias and heuristics which are context dependent. Moreover, practical implications to nudge behaviour in consumption domains are the fact that consumers tend to rely on the status quo bias considering any deviation as a loss or the fact that consumers tend to grant value to items already possessed by someone else that they do not own (endowment effect). The knowledgeable use of these tools has remarkable effects on different issues relating to product choice healthy eating, financial decision making and sustainable consumption.[104]

It must be noted that notwithstanding the apparent appeal of the nudging theory and its practical applications in many different policies, both in the US and UE, concerns are still in place: libertarian paternalism seems to be inadequate as a guiding ethical framework because it fails to recognize how being nudged fully affects different human capabilities.[105] Critical scholars noted that human preferences are not stable as the theory of nudging tends to affirm, and an alternative, it proposed an 'active choosing by design', as a default rule for nudges, where social learning and related development consequences are relevant.[106]

2.2 … or to manipulate digital consumers

Ultimately, architectural design is a source of power.[107] Design induces consumers to agree to something they might not have chosen with another type of design. It is difficult – if not impossible – to determine what authentic consumer preferences are, how they express their preferences, and what actions, or decisions, would align with their preferences.

Designs can have a fair (persuasive) purpose. However, they can also be inspired by other purposes, including unfair intentions: in this way, what was described as a nudging technique can be transformed, updated, and

[103] See the findings of the World Bank, 'Mind, society, and behavior' (World Development Report), 2014.

[104] See Lucia A. Reisch, Min Zhao, 'Behavioral economics, consumer behaviour and consumer policy: state of the art' (2017) 1(2) Behavioural Public Policy 190-206.

[105] Brett M. Frischmann, 'Nudging Humans' (2019) <https://ssrn.com/abstract=3440791> accessed 2 November 2022.

[106] ibid

[107] Ryan Calo, 'Digital Market Manipulation' (2014) 82(995) Geo Wash L Rev 1021; Justin Hurwitz, 'Designing a Pattern, Darkly' (2020) 22(57) N C J L & Tech 67-68.

targeted in potentially elusive or manipulative practices. Empirical studies demonstrated that in digital context, companies can discover how changes in interfaces and product designs will impact consumer choices and behaviour.[108]

Concisely, the intent is to introduce the critical distinctions subtended to the different aims of the practices.

Here is the main difference between the original meaning of nudging and the 'pathological' interpretation.

Following the definition expressed by the European Data Protection Supervisor (EDPS),[109] with the Opinion 3/2018 relating online manipulation and personal data:

'manipulation also takes the form of microtargeted, managed content display which is presented as being most 'relevant' for the individual, but which is determined in order to maximize revenue for the platform. This is akin to the 'secret menus' used to steer users of ecommerce sites and the 'dark patterns' used to dissuade decisions less desirable from the platform's perspective (such as declining to add additional items, like insurance, to a shopping cart)'.[110]

In the same way as nudges, manipulation often works by leveraging cognitive biases. However, conversely from it, a manipulative practice aims at changing the way the user would have acted in the absence of it. It can be challenging to understand when nudging ends and manipulation starts when considering how options are selected, arranged, and affect how people understand and respond to them, even affecting conscious awareness. Following Cass Sunstein's words, an influence is manipulative 'to the extent that it does not sufficiently engage or appeal to [the target's] capacity for reflection and deliberation'.[111] Manipulative practices are often targeted towards 'cognitive, emotional, or other decision-making

[108] Brian Christian, 'The A/B Test: Inside the Technology That's Changing the Rules of Business' (Apr. 25, 2012), WIRED <https://www.wired.com/2012/04/ff-abtesting/>. For A/B testing the Authors mean to allow seemingly subjective questions of design – colour, layout, image selection, text – to become incontrovertible matters of data-driven social science.

[109] The European Data Protection Supervisor (EDPS), 'Opinion 3/2018 on online manipulation and personal data' (19 March 2018), 9, <https://edps.europa.eu/sites/edp/files/publication/18-03 19_online_manipulation_en.pdf> accessed 20 December 2019.

[110] ibid

[111] Cass Sunstein, *The Ethics of Influence: Government in The Age of Behavioural Science* (Cambridge University Press 2016) 82.

vulnerabilities.[112] Hidden influence and exploitation of vulnerabilities are the primary means of manipulation.

Unlike persuasion, with manipulation one takes control over users. Legally speaking, the existing fine line is similar to the distinction between 'legitimate influence' and 'illegal distortion' of the average consumer's behaviour under the UCPD.[113]

Under the pressure of manipulation, users lose their capacity for self-government, and manipulation 'undermine or disrupt the ways of choosing that they would critically endorse if they considered the matter in a way that is lucid and free of error'.[114]

Spenser describes the evolution in how manipulation is considered, distinguishing different eras: the pre-digital era, the digital era, and the current digital era. Concerning the context of data-driven technologies, users are efficiently engaging in manipulative practices, as well as they are the target of digital surveillance, and without difficulties their vulnerabilities and regular decision-making process are identified.[115]

Behavioural advertising is a subject of particular interest for the application of manipulation techniques.[116] For example, the fact that Facebook can monitor the content and tone of user interactions is functional to targeting their young community (e.g. teenager users) with advertisements. Online behavioural advertising, or interest-based advertising, has represented the object of study and attention of different regulatory authorities. In the US, the Federal Trade Commission (FTC), an

[112] Daniel Susser, Beate Roessler, Helen Nissenbaum, 'Online Manipulation: Hidden Influences in a Digital World' (2019) 4(1) Geo L Tech Rev 27.

[113] Jan Trzaskowski, 'Behavioural economics, Neuroscience, and the Unfair Commercial Practices Directive' (2011) Journal of Consumer Policy 377.

[114] Allen Wood, 'Coercion, Manipulation, Exploitation', in Christian Coons, Michael Weber (eds.), *Manipulation: Theory and Practice* (Oxford University Press 2014) 17.

[115] Karen Yeung describes the problem as 'hypernudging'. See Karen Yeung, 'Hypernudge: Big Data as a Mode of Regulation by Design' (2017) 20 Info Comm & Soc'y 118.

[116] Advertising plays vital role in an ideal competitive free market: informed consumers can effectively select products and services among the alternatives, thus ensuring supply meets demand and prices adjust accordingly. There are also opposite views, following which advertising are increasingly aimed at circumventing consumers. Vance Packard, famously charged the advertising industry with 'motivation analysis', psychological and psychoanalytical means to exploit 'hidden weaknesses and frailties' to appeal to non-rational and subconscious mental processes in service of marketing ends. Lastly, a moderate position suggest that advertising can serve a useful function even though outcomes are deeply problematic. Vance Packard, *The Hidden Persuaders* (Pocket Books 1959).

independent federal agency whose main scope are the protection of consumer and competitive markets, defined it as tracking a consumer online activities over time to deliver advertising targeted to the consumer's interests. The tracked activities are searches conducted, web pages visited and content viewed.

US regulation of the phenomenon is mainly based on industrial self-regulation by FTC principles. Likewise, in the EU, the complex online advertising ecosystem which involves a multiplicity of actors (e.g. publishers, advertising intermediaries, such as advertising networks; supply-side and demand-side platforms; data management companies), has recently been studied by the European Commission, mainly to understand the compatibility with legal provisions on consent, contained in the Charter of Fundamental Rights and in a multiplicity of EU secondary legislation (GDPR; Service Act; e-privacy; Digital Content Directive, see more in Chapter II).[117]

To conclude, a popular example of the criticalities encountered when distinguishing the various levers of influence and persuasion from manipulation in advertising is the terrain of the psychographic profiling used influence elections after the Cambridge Analytica scandal. In March 2018, the political services firm Cambridge Analytica, employing, in turn, the company Global Science Research (GSR) to generate vast repositories of digital user profiles, had improperly used Facebook's advertising social network to exercise influence in the 2016 U.S. presidential election.[118]

The approach employed was different to traditional mass advertising: Cambridge Analytica personalized messages in a range of media from direct mail to online cookie driven, to targeting, to social media banners, and even to set up televisions. Cambridge Analytica's sophisticated

[117] The study is written by Giovanni Sartor, Francesca Lagioia, Federico Galli, (requested by the JURI committee of the EU Parliament), 'Regulating Targeted and Behavioural advertising in digital services (How to ensure users' informed consent)' (2021) <https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2021)694680>. The study addresses the regulation of targeted and behavioural advertising in the context of digital services.

[118] These repositories were initially considered a result of a personality quiz, named 'this is your digital life' (2014), administered by Aleksandr Kogan, a lecturer in the Department of Psychology at the University of Cambridge and the head of GSR. Carole Cadwalladr, Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' (Mar. 17, 2018) Guardian, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influenceus-election>. Cecilia Kang, Sheera Frankel, 'Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users' (Apr. 4, 2018) NY Times.

operation consisted of transforming psychographic profiles, mainly acquired by online measures, such as Facebook 'likes',[119] to targeted messaging, where the tailoring messages correspond to the specific personality traits of their recipients.

Technological advances give reason to believe that efforts like these will continue to evolve (section 3.3).

2.3 The phenomenon of dark patterns (see Chapter II, section 2)

All choice architectures can potentially constitute dark patterns when they have different aims from the one to honestly nudging consumers toward a decision in their best interest.

Based on manipulation, several different techniques exploit people's emotions or constitute tactics based on lies, false promises, and pressure.[120]

Given that the phenomenon of dark patterns is central to this analysis, it will be extensively described in section 2 of the Chapter II, to maintain the unitarity of the study-case focus.

By way of example of the analysed phenomenon, the nagging tactics represent one of the categories of dark patterns which shows a distinctive trait: unlike the other types of dark patterns, it does not target a specific consumer vulnerability.[121] It is substantially a repetition of a request addressed to the user to do something the company prefers them to do. The persistence of the request can, ultimately, lead the consumer to satisfy the request, and depending on the type of consumer nagging can help or hinder them. This happens, for example, every time Google prompts users who have disabled 'location services' to consider enabling the feature.

Nagging practices harm consumers and warrant timely intervention, mainly because they concern the validity of consumer consent. Under conditions of frequent notifications or continuous reminders consumer self-determination and freedom of choice could be threatened. They are all

[119] Facebook does not allow marketers to target advertisements based on psychological traits directly, but it does so indirectly by offering the possibility to target users based on their Facebook Likes.

[120] Marcia Baron, 'Manipulativeness' (2003) 77 Proc & Addresses Am Phil Ass'n 37.

[121] Alison Hung, 'Keeping consumers in the dark: addressing 'nagging' concerns and injury (Notes)' (2021) 121 Columbia Law Review 2483-2520.

pragmatic situations in which consumer attention is under pressure. Some considers the situation as 'Attentional Theft'.[122]

Other effects of nagging, predominantly indirect, can affect privacy or provoke implications for antitrust as it can lead consumers to disclose more personal data than necessary for the services (see Chapter II section 2).

Above all, this anticipation is finalised to give account of the research attempts to provide new computer-based systems for evaluating digital fairness of the most influential website across the Member States. In this sense, Claudette is a perfect example of an experimental project developed by the European University Institute in Florence, which can partially automate the checking of websites.[123] The original aim of the program was to investigate whether artificial intelligence could be trained to contribute helping consumers to check the terms of service for unfair terms[124].

As a preliminary consideration, notwithstanding the valuable efforts of empirical research, the actual knowledge of unfair terms and architectures in the Digital Age is still limited and requires steps forward.[125]

2.4 Manipulative design and unexplored pitfalls for the information approach

Legal concerns emerged when seeking to regulate new data-driven scenarios through the foundational European information approach (see section 1.3).[126]

The limits of the pivotal principle are manifest in online marketing, where novel business-consumer negotiation circumstances exist. Consequently, 'these situations give rise to their rationales for information provisions, given that the consumer is dealing with a remote trader, about whom he may know very little:

[122] Tim Wu, 'Blind Spot: The Attention Economy and the Law' (2017) 82 Antitrust L J 771, 778.

[123] Claudette is, in substance, a machine learning-powered analysis of consumer contracts and privacy policies. It is available at <http://claudette.eui.eu/index.html> accessed 10 October 2023.

[124] Francesca Lagioia, Agnieszka Jabłonowska et al, 'AI in search of unfairness in consumer contracts: the terms of service landscape' (2022) 45 Journal of consumer policy 481, available at <https://hdl.handle.net/1814/74834> accessed 10 September 2023. See also Cristina Poncibò, 'Research protocol/Methodology for UCTD' (forthcoming 2024) 102 ERCL.

[125] Caterina Gardiner, *Unfair Contract Terms in the Digital Age* (EE Elgar 2022).

[126] See Helleringer, Sibony (n 25) 629-30.

at the very least, he needs to have contact details for the trader and information about the product or services being supplied'.[127]

Depending on the design of digital infrastructures, traders must disclose information in several areas, such as information regarding the contract terms. However, also the process of personal information and the use of cookies.[128] Due to the nature and the potential consequences of digital architectures design on consumer behaviour, it is not apparent that the variety of mandatory disclosures provided by European consumer law effectively protect them and preserve their autonomy.

What seems to be the cause of the 'trap' is that, even if the digital architecture design is legally complaint with disclosure obligations, the same design can also injure consumer authentic free will and consequently their actions. What is more is that, with exceptions for a limited number of policies focused on design, like food law (e.g. food labels), there is still limited specific guidance for the consumer's protection in situations of architectural nag or manipulative design techniques.[129]

To go further on the way the technological features impact on traditional approach, it should be considered the transactions between traders and consumers settled in online platforms. Prudent position suggested considering the power and availability of information of the recipient of the service, as it is not always evident the parties, identities and legal status:[130] this uncertainty doubts the applicable legal framework to the supply contract. Taking into account Art. 6 *bis* of the CDR, as amended by the Modernization Directive, it would be essential to strengthen information requirements about the identity of goods/providers, to know the role of the intermediary (online platform), as the platform can bear some of the duties from the supply contract; and to identify if they are buying goods or submitting services from a trader or from a non-trader.[131]

[127] Scholes (n 11) 213.

[128] Ognyan Seizov, Alexander J. Wulf, Joasia Luzak, 'The Transparent Trap: A Multidisciplinary Perspective on the Design of Transparent Online Disclosures in the EU' (2019) 42 J Consumer POL'y 149. The authors' arguments aim at convincing EU policymakers to (re-)consider the importance of information design because it could improve the effectiveness of information duties.

[129] This situation often allows online traders to blur the lines between the mandatory information provisions and their disclaimers, which increase the amount of information consumers must read.

[130] Guido Smorto, 'La tutela del contraente debole nella platform economy' (2018) 158 Giornale dir lav relaz industriali 423.

[131] Montinaro (n 40) 55.

Consequently, establishing the specific nature of platform is essential. Practically speaking, the Digital Service Act,[132] which will be further analysed in Chapter II, determines the correspondence between different online players and their role, size, and impact on the online ecosystem (Art. 5 DSA). It introduces a comprehensive new set of rules for online intermediary services about how they must design their services and procedures. The new rules include new responsibilities to limit the spread of illegal content and illegal products online, increase the protection of minors and give users more choice and better information.

Therefore, also Art. 7 f) of the UCPD as amended by the same Modernization directive states that, in order to avoid a sanction for unfair practice, the party offering the product by using a platform is obliged to disclose whether or not it is acting as a trader 'on the basis of the declaration of that third party to the provider of the online marketplace' (Art. 7, f).[133] In cases where the platform plays a role of mere intermediary, with due diligence obligations, this must be communicated to the consumer: following recital 19 of the Digital Service Act (DSA) online platforms can act as 'mere conduit', 'caching' and 'hosting' entity.[134] Extensively, recital 19 states:

'in view of the different nature of the activities of 'mere conduit', 'caching' and 'hosting' and the different position and abilities of the providers of the services in question, it is necessary to distinguish the rules applicable to those activities, in so far as under this Regulation they are subject to different requirements and conditions and their scope differs, as interpreted by the Court of Justice of the European Union' (recital 19, DSA).

All online intermediaries will also have to comply with wide-ranging new transparency obligations to increase accountability and oversight, for example, with a new flagging mechanism for illegal content.

[132] Parliament, Council Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277.

[133] Parliament, Council Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council' ('Unfair Commercial Practices Directive') [2005] OJ L 149, 22-39.

[134] Parliament (n 65).

DSA creates unprecedented public oversight of online platforms across the Union, both at National and EU level. The expected effect of the DSA enforcement will be to create comprehensive new obligations for online platforms to reduce harm and counter risks online. It introduces strong protection for user rights online and places digital platforms under a unique new transparency and accountability framework. These rules will give users new protections and businesses legal certainty across the whole single market. DSA is a global first-of-a-kind regulatory toolbox and sets an international benchmark for a regulatory approach to online intermediaries.

Proactive critics arise when considering the findings of behavioural economics and psychological research on consumer law.

Empirical evidence of behavioural economics shows a new policy model could be more efficient by taking into account data from the study of heuristics, biases and situational dependency. A regulation structured in this way could guide consumers to make better decisions: nudges are defined as low-cost, choice-preserving, empirically informed approaches to regulatory issues, including disclosure requirements, default rules, simplification and use of salience and social norms.[135]

Attempts to consider these new insights already exist in regulatory processes. In the mid-2000s, for example, public authorities became interested in adopting nudges as additional behavioural based policy techniques in a variety of fields, such as healthy eating and standard terms in consumer contracts.[136] This type of regulation seems to be more time-saving, group-specific and problem-tailored solutions. The nudge-based policy can also be communicated so people can be aware of it. Statistics demonstrate that in many countries, people approved such tools on average and depending on the policy goal: 'people believe that if a nudge has legitimate goals and they think that it fits with the

[135] Lucia A. Reisch, John B. Thøgersen, 'Behaviorally informed consumer policy: Research and policy for 'humans', in Margit Keller, Bente Halkier, Terhi-Anna Wilska, Monica Truninger (eds), *Routledge handbook on consumption* (Routledge 2017) 242-253.

[136] Organization for Economic Co-operation and Development (OECD), '*Behavioural insights and public policy. Lessons from around the world*' (2017) <https://www.oecd.org/gov/regulatory-policy/behavioural-insights-and-public-policy-9789264270480-en.htm> accessed 27 July 2022; see also Lucia A. Reisch, Cass R. Sunstein, 'Do Europeans like nudges?' (2016) 1(4) Judgment and Decision Making 310-325.

interest or value of most people, they are overwhelmingly likely to favour it'.[137]

Apart from the consideration of the design as a regulatory goal to be disciplined, the new rules on modernizing consumer law, and in particular the rules on recommender systems expressed by Art. 2 of the DSA, implicitly recognized that the way algorithms are designed and used to rank goods or services may affect consumer autonomy.[138] The fact is that the content made available to each consumer could be differentiated in light of several parameters, including the use of profiling and personalized techniques. Often, the 'opacity' of the criteria used to arrange the results of the online search prevents the user from understanding the logic recommender systems applied, representing one of the significant features of what Frank Pasquale defines as 'black box society'.[139]

3. New trajectories to advance legal research

Alongside the scenario sketched out on the previous pages, with particular attention to the potentialities of technologies in exploiting consumer psychological attitudes, it is essential to individualize the emerging legal trajectories to set the research framework. Premises are both methodological and substantial.

On the methodological side, a twofold assumption is adopted: the need to investigate consumer autonomy through a regulatory perspective instead of the much more limited legislative one, and the consequent need to

[137] Lucia Reisch, Min Zhao, 'Behavioural economics, consumer behaviour and consumer policy: state of the art' (2017) 1 Behavioural Public Policy 201.

[138] Art. 2 of the Digital Service Act (n. 65) states at lett. r): «'advertisement' means information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes and displayed by an online platform on its online interface against remuneration specifically for promoting that information». At lett. s) DSA defines: «a 'recommender system' means a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed».

[139] Montinaro (n 40).

consider insights from other disciplines necessary to acquire a broad, inclusive perspective to investigate the topic.[140]

The leading governance scholarship defines regulation as intentional attempts to manage risk or alter behaviour to achieve pre-determined goals.[141] Regulation can also be pursued by non-state actors, by a single actor, and by soft-regulatory tools, through several strategies (not only legal ones) to influence some individual behaviours.

Adopting the lens of regulation will ultimately mean to include policy and governance tools that can be unfamiliar to lawyers.

Scholars of Science and Technology Studies (STS) have long recognized the significance of material object design on social behaviour,[142] and recently, a leading legal scholar used the term 'techno-regulation' to describe these instruments in a digital environment. The initial idea went so far that recent scholars discussed the ongoing path

[140] Regulatory instruments can be classified in many ways (Bronwen Morgan, Karen Yeung, *An Introduction to law and regulation: Texts and Materials* (Cambridge University Press 2003). A popular starting point for analysis is the Lessig's fourfold taxonomy of modalities of control that distinguishes between law, markets, social norms, and code (Lawrence Lessig, *Code and other laws of Cyberspace* (Basic Books 1999), and which can be understood as a variant of the tripartite typology of social coordination mechanisms consisting of hierarchy, markets, and networks.

[141] In recent years, regulation has emerged as one of the most distinct fields of study in social sciences, both for policy-makers and for scholars who require a theoretical framework that can be applied to any social sector. Roger Brownsword, Eloise Scotford, Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford Handbooks 2017; online ed, Oxford Academic, 1 Sept. 2016); Karen Yeung, 'Towards an Understanding of Regulation by Design', in Roger Brownsword, Karen Yeung (eds.), *Regulating Technologies* (Oxford University Press 2008) 79-94; Karen Yeung, 'Can We Employ Design-Based Regulation While Avoiding Brave New World?' (2011) 3(1) Law, Innovation and Technology 1-29; Karen Yeung, 'Design for Regulation', in Jeroen van den Hoven, Ibo van de Poel, Pieter E. Vermaas (eds.) *Handbook of Ethics, Values and Technological Design* (Springer, 2015) 447; Karen Yeung, 'Hypernudge': Big Data as a Mode of Regulation by Design' (2017) 20(1) Information, Communication & Society 118-136; Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (May 23, 2017) TLI Think! Paper 62/2017, Regulation & Governance, forthcoming, King's College London Law School Research Paper No. 2017-27, <https://ssrn.com/abstract=2972505> accessed 20 July 2022; Julia Black, 'Learning from Regulatory Disasters' LSE Law, Society & Economy (2014) Working Papers 24/2014; see also Roger Brownsword 'Code, Control, and Choice: Why East Is East and West Is West' (2005) 25(1) Legal Studies 1-20; Roger Brownsword, 'Technological Management and the Rule of Law' (2016) 8(1) Law, Innovation and Technology 100-140.

[142] Jaap Jelsma, 'Innovating for Sustainability: Involving Users, Politics and Technology' (2003) 16 Innovation 103; for a general frame see: Yeung (n 115), 1-29.

from «code is law»[143] to «law is code»,[144] meaning with the advent of advanced technologies (e.g. blockchain technology), code is assuming an even more vital role in regulating people's interactions over the Internet, and law is defined as code.

As a general observation, regulation by design is a crucial and debated current topic. A regulatory function has been attributed to the 'design' both by public law and private law purposes. Securing adherence to the rule of law is a perennial challenge in every society. This is the reason for an extensive discussion of the opportunity to include *ab origine* the rule of law into a technological design since the very beginning.[145] The most common application of this approach concerns private law aspects (see Ch. II and III).

In 'algorithmic regulation', for example, algorithms are used to impact on consumer rights deeply.[146] After all, a variety of legitimate design-based approaches for achieving social goals already existed.[147] Internet studies and governance debates often take as a starting point the famous Lessig's

[143] With the advent of digital technology, code has progressively established itself as the predominant way to regulate the behaviour of Internet users. Yet, while computer code can enforce rules more efficiently than legal code, it also comes with a series of limitations, mostly because it is difficult to transpose the ambiguity and flexibility of legal rules into a formalized language which a machine can interpreted.

[144] Primavera De Filippi, Samer Hassan, Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code (December 5, 2016) 21(12), in Primavera De Filippi, Samer Hassan (eds), Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. First Monday (special issue on 'Reclaiming the Internet with distributed architectures), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3097430> accessed 8 May 2023.

[145] Monika Zalnieriute, Lyria Bennett Moses, George Williams, 'The Rule of Law "By Design"?' (2021) 95(5) Tulane Law Review 1063-1101. The Authors ask whether fostering the rule of law 'by design' – which envisages technological solutions non-compliant with the rule of law requirements – can promote or guarantee the rule of law in practice.

[146] Lena Ulbricht, Karen Yeung, 'Algorithmic regulation: A maturing concept for investigating regulation *of* and *through* algorithms' (2021) 16(1) Regulation & Governance 3-22); Karen Yeung, Lee A. Bygrave, 'Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship' (2022) 16(1) Regulation & Governance 137-155.

[147] For an in-depth discussion, see Karen Yeung, 'Towards an understanding of Regulation by Design', in Roger Brownsword, Karen Yeung (eds), *Regulating technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart 2008) 79-107.

idea considering architecture (or code) as one of the sources of the 'regulatory tool-box' to realize a collective or social outcome.[148]

Subsequently, modern studies explore the interface between law, regulatory governance, and emerging technologies.[149] Nowadays, radical rethinking of the relationship between them disregards the concept of technology as an issue of particular interest for institutions, and considers modern technologies as doubly significant, both as primary targets for regulation, and as potential tools to be used for legal and regulatory purposes.[150]

Examples where the current regulation accepted and implemented the role of technology as a regulatory function already existed: Arts. 24, 25 and Art 28 of the General Data Protection Regulation (GDPR),[151] which provides the 'data protection by design and by default' requirement, imposing legal obligations on data controllers to 'hard wire' data protection norms into information systems development, thus mandating the use of 'design-based' regulatory techniques.

Consequently, adopting the lens of regulation implies choosing a method to reach the findings from non-legal disciplines, and to understand the interconnection between their methods with the common aim of managing social risks.

The benefits of the recourse to interdisciplinary are also evident when considering the empirical findings of behavioural economics, which introduce considerations to subvert the European information paradigm, traditionally served to foster the e-commerce market and protect cross-border transactions. From this perspective, the regulation by design could be an effective tool to question the assumptions of what would guarantee transparency and effective provisions when online information and

[148] Particularly there are two hallmark writings in internet studies: Lawrence Lessig, *Code and other Laws of Cyberspace* (Basic Book 1999); and Lawrence Lessig, 'The Law of the Horse: What Cyberlaw might Teach' (1999) 113 Harvard Law Review 502.

[149] Besides the others: Mireille Hildebrandt, Antoinette Rouvroy (eds), *Law, Human Agency and Autonomic Computing. The Philosophy of Law meets the Philosophy of Technology* (Routledge 2011); Yeung (n 115); Lee A. Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4(2) Oslo Law Review, <https://ssrn.com/abstract=3035164> accessed 20 November 2022.

[150] Roger Brownsword, *Rethinking Law, Regulation and Technology* (EE Elgar 2022).

[151] Parliament, Council Regulation 2016/679 of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] *OJ L* 119.

advertising are governed by such web designs and technologies, which, in the worst hypothesis, configure dark patterns.

In future perspective, other potential insights can come from the emerging area of studies on 'law and emotion', which has been suggested deserves to join the family of interdisciplinary approaches.[152] Scholars from diverse fields have begun to study the intersection of emotion and law because the idea that reason and emotion are cleanly separable – and that law rightly privileges and admits only the former – is deeply ingrained. Law and emotion scholarship proceeds instead from the belief that the legal relevance of emotion is both significant and deserves (and is amenable to) scrutiny.

From a substantial point of view, it is preliminary essential to identify the multiplicity of the legal features of data-driven technologies before focusing on the specific dark patterns case-study (Chapter II).

These features will be explored in general terms before going into details with the following sub-sections (sections 3.1, 3.2., 3.3).

The first factor is theoretical, and it consists of avoiding thinking of consumer transactions as part of contract law.[153] Considering, for example, data autonomy, the need for data to be protected must be balanced with the need for it to be accessible and shareable. Consequently, due to the different functions of data, a set of critical principles will grant individuals a legal right to data autonomy, including a right of ownership over data obligations on institutions to share standardized and interoperable data with third parties safety.

Consumer data value has received an increasing level of attention for privacy control. Thus, the second factor of the analysis emerges the interaction between different policies involved. The foremost is the intersection between consumer law and data protection law since data

[152] Terry Maroney, 'Law and Emotion: A Proposed Taxonomy of an Emerging Field' (2006) 30 Law Hum Behav 119-142. See Susan Bandes (ed), *The passions of law* (New York University Press 1999); see also Kathryn Abrams, 'The progress of passion' (2002) 100 Michigan Law Review 1602; Neal Feigenson, 'The role of emotions in comparative negligence judgments' (2001) 31(3) Journal of Applied Social Psychology 576; Heidi L. Feldman, 'Foreword: Law, psychology, and the emotions' (2000) 74 Chicago-Kent Law Review 74 1424; Sanger Sanger, 'The role and reality of emotions in law' (2002) 8 William and Mary Journal of Women and the Law 107. An open question remains whether 'law and emotion' is rightly considered a 'field' or 'movement', or whether theoretical and empirical explorations of the law-emotion interaction are merely a content-based point of intersection among various established interdisciplinary fields.

[153] Scholes (n 11), 213-237.

ultimately is information. Choices enable platforms to generate attention and capture data, the primary commodities of the digital economy. With attention and data, platforms can exploit their users' cognitive vulnerabilities through design choices meant to guide individuals towards behaviours sought by the platform.

This is not the sole intersection between different policies. Competition law is also at stake, particularly after the recent ECJ judgement in case C-252/21 of 4 July 2023 stated that a national competition authority could find, in the context of the examination of an abuse of a dominant position, that the GDPR has been infringed (see Ch. II).[154] Digital manipulation implicates antitrust law when a firm uses a product designed to manipulate, or coerce, consumers, rather than merely persuade them. There is a fine line between legitimate forms of persuasion and the exercise of undue influence or even coercion over consumers. Consequently, the enforcement phase is complicated by the duty to examine how allegations of coercion might apply to digital manipulative practices: the investigation of the adequate protection of autonomy before the potential threats of online manipulation implies distinguishing persuasive (competitive) from coercive (anticompetitive).[155]

Moreover, the overlapping effect exists between different policies, and provokes other essential effects: the blurring of lines between private and public law, and between different taxonomies (section 3.2).

Thirdly, the current regulatory scenario must deal with the broad phenomenon of personalization. Powerful algorithms can exploit knowledge about specific and personal consumer vulnerabilities and emotional tendencies. The fact that digital technologies allow not only knowledge of consumer preferences and profiles but also the inferred psychological states, vulnerabilities and personal misperceptions can give rise to personalized legal tools (section 3.3).[156]

[154] Case C-252-21 *Meta Platform and Others* (General terms of use of a social network) [2023] EU:C:2023:537.

[155] Gregory Day, Abbey Stemler, 'Are Dark Patterns Anticompetitive?' (2020) 72 Ala L Rev 1. The Authors show that digital manipulation erodes users ability to act rationally, which empowers platforms to extract wealth and build market power without doing so on the merits. In fact, as antitrust law enforcers conventional privacy as a benefit of competition, it should further promote decisional privacy. This would increase consumer welfare and generate competition in digital markets and fill in pressing gaps in consumer protection laws.

[156] Christopher Burr, Nello Cristianini, 'Can machines read our minds?' (2019) 29 Minds and Machines 494.

3.1 The research overlapping area: blurring the line between legal policies

The cross-cutting nature of data has prompted a new twist in the relationship between data protection, consumer law, and competition law. This leads to the convergence of different legal domains and new points of tension between them. A growing volume of regulatory policy documents testifies this trend (see Chapter II).

Besides their specific goals, competition law, consumer law, and data protection law serve the common aim of protecting the internal market differently way. Competition and consumer law aim at enhance social welfare, while data protection law originates in fundamental rights protection.

This individual rights protection is not instrumental to achieving other goals, such as enhancing social welfare. Instead, it is inextricably linked to the protection of human dignity. While competition and consumer laws regulate the use of data – only to the extent that it affects competition and consumers – data protection regulates the collection and use of personal data in general.

Data is crucial for a company to achieve commercial success, as it is routinely used to offer products and services to customers. This also makes data collection and use subjective to competition and consumer law. At the same time, personal data is also a fundamental right, as outlined in Art. 8 of the EU Charter of Fundamental Rights (hereafter: EU Charter).[157] Indeed, the term 'consumer privacy' is common in US literature, and in some jurisdictions the term 'consumer data protection' is used as well.[158]

In modern markets, where many companies offer services, consumer and data protection law can complement each other. Data protection law, in recent case law, contributes to informing the interpretation of consumer law: consumer rights become functional to challenge the excessive collection of their personal data and tackle data protection infringements. The interplay of data protection law and consumer protection law provides exciting opportunities for a more integrated vision of 'data consumer law'

[157] Irene Kamara, Eleni Kosta, 'Do Not Track initiatives: regaining the lost user control' (2016) 6(4) Int Data Priv Law 276-90.

[158] Kash Leng Ter, 'Information Management: Towards Consumer Data Protection Legislation in Singapore' (2012) 24 Singap Acad Law J 143.

and it deserves specific analysis to frame the current research inquiry about autonomy (section Chapter II).[159]

Nevertheless, critical issues are still numerous. In the digital environment, where almost any data can be linked to an identifier, the distinction between what constitutes personal data and what remains non-personal data – and therefore not subject to the scrutiny of stringent data protection rules – is often difficult to trace.

Many lawyers have already defined the General Data Protection Regulation (GDPR) as the 'law of everything' because it applies to almost any collection and use of data. As a result, in any data-related enforcement action by competition or consumer authorities – or any other authority for that matter – data protection rules apply.[160]

The relationship between consumer and data protection law is complex, particularly within the EU's online environment. While there are significant similarities between their respective sources, tools and purposes, there are also arguable differences between the two policies, which will be further exposed (see Chapter II).

An exemplary matter of the overlapping phenomenon is online advertising is the usual setting in which firms design dark patterns to obtain personal consumer data. Within the digital era, the protection of EU consumer personal data has become increasingly important, as the individual data is often exposed, shared, and transferred to sellers and third parties. To target advertising and offer personalized recommendations or customizing products and services, based on consumer preferences, weaknesses, and psychological insights. Given the increased need to protect consumers from unlawful advertising, the discipline of online advertising shows the (problematic) interaction between EU data protection law and EU consumer law.[161] Consumer law could offer an

[159] Natali Helberger, Frederik Zuiderveen Borgesius, Augustin Reyna, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54(5) Common Market Law Review.

[160] Parliament, Council, Regulation 2016/679 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 (General Data Protection Regulation) [2016] *OJ L* 119.

[161] Regarding targeted advertising regulation, Erica Palmerini underlined the limit of GDPR regulation, which is truly applicable only to algorithmic decisions and not to algorithmic manipulative practice. See Erica Palmerini, 'Algoritimi e decisioni automatizzate. Tutele esistenti e line evolutive della regolazione', in Luis Efrén Rios Vega, Lucia Scaffardi, Irene Spigno (eds.), *I diritti fondamentali nell'era della* digital mass surveillance (Editoriale Scientifica 2021), 209, 236.

additional layer of protection in cases of personal data breaches by the AdTech industry.

Lastly, from a competition law perspective, although personal data cannot be reduced to a mere commodity or consideration for a service, in some instance, the amount of personal data collected from individuals by a service provider (as in two-sided markets, such as social media services) can be compared to a price. From this perspective, competition, consumer, and data protection laws aim to empower individuals to make choices on price and quality (where personal data can be both a substitute for price and a characteristic of quality) and address power asymmetries.

Competition law creates a choice for consumers on price and quality to secure lower prices and higher quality of products and services. Consumer law aims to protect consumers (generally considered the weaker party vis-à-vis a business) by guaranteeing them a choice in terms of price and protecting them by imposing quality and safety standards. For this reason, it has been observed that competition law and consumer law mutually reinforce each other. Data protection, in turn, adds layer of protection, safeguarding individual control over personal data and choices.

3.2 The effects of disruptive technologies on long-established legal taxonomies

Over the years, legislative typification and normative archetypes have been harshly challenged by the phenomena of digitalization and globalization, which have increased the complexity of law.[162]

A mutual bonding between the development of traditional normative taxonomies and digital impact produced a disruptive effect on how legislators have reduced the complexity of real social situations into predetermined standard models and categories. The digital world adds a new immaterial dimension and creates unexplored situations in law with new opportunities for consumers.[163]

When observing the structure of the General Data Protection Regulation (GDPR),[164] based on the 'one-fits-all design' of legal norms,

[162] Complexity is the opposite of simplification: Pompeu Casanovas, Ugo Pagallo, Giovanni Sartor, Gianmaria Ajani (eds.), *AI Approaches to the Complexity of Legal Systems: International Workshops AICOL-I/IVR-XXIV, Beijing, China, September 19, 2009 and AICOL-II/JURIX* (2009) 6237 Revised Selected Papers.

[163] On the main features of digital law see: Giovanni Pascuzzi, *Il diritto dell'era digitale* (il Mulino, 2020).

[164] Parliament, Council Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of

which includes many different cases into a sole Regulation, a certain degree of imprecision and difficulty to guarantee protection in different cases emerges (see Ch. III).[165]

Normative models work on the base of approximation and can lead to regulatory errors, inequalities, and inefficiencies. To avoid unequal treatment and to ensure a higher degree of individual fairness, an opposite approach can be achieved at the price of reduced legal certainty or higher complexity costs.

Examples are numerous, mainly emphasizing the inadequacy of traditional categories to cope with new legal issues or underlining the blurring of lines between two or more traditional categories. Typification is undoubtedly necessary in law nonetheless it is a characteristic trait of the Western legal tradition systems.[166] Only recently, scholars focused proactive efforts to search for new categories and propose legal reasoning based on new foundational structures of law (see section 3.3), in the direction of the already mentioned law 3.0 scenario.

A recurrent example comes from the field of property rules applicable to data. It shows the controversial discussion in legal doctrine regarding the existence of an 'ownership' right to data.[167] Data is a non-rival resource. However, can also have an excludable nature as its use can be restricted, denying access. The concept of exclusivity poses several questions and concerns about 'data rights': there are concerns about what types of data (namely, information) would be the object of exclusivity, as well as concerns about the fact that data can be reproduced, used, and distributed as often desired without the data owner losing the same opportunity to reproduce, use and distribute the data.

Another specific issue involved in dark patterns debate can be anticipated: the blurring of lines between advertising and information.

'Among the practices that can threaten consumer autonomy are forms of covert advertising, which frequently occur in online platforms. These practices are made possible by the fact that the boundaries between genuine information (or recommendation) and advertising have become

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[165] Martin Ebers, Karin Sein (eds.), *Privacy, Data Protection and Data-driven Technologies* (Routledge forthcoming 2023).

[166] Lawyers daily work with taxonomies. See Giovanni Pascuzzi, *Il problem solving nelle professioni legali* (il Mulino 2017).

[167] On the issue see Sjef van Erp, 'Ownership of data: the numerus clausus of legal objects' (2017) 6 Brigham-Kanner Property Rights Conference Journal 235-257.

blurred in the context of online interactions between traders and consumers. Digital platforms tend to take advantage of this opacity'.[168]

There are many circumstances that do not clearly state the fact that communication has commercial intent. This makes the practice unfair under the UCPD provisions, according to which any form of commercial communication must be identifiable as such by the recipients of the communication.

About this situation, the Unfair Commercial Practices Directorate set up by the Italian Autorità Garante della Concorrenza e del Mercato (AGCM) has underlined the difficulty of allocating the responsibility for performing the duty of advice about the intent to advertise: it is important to specify if it is the supplier or the influencer that have to advise about the intent to advertise, and the potential role of the platform to guarantee transparency about it.[169]

3.3 Personalized advertising, and services… and 'personalized law'

The continuous growth and impact on consumer choices of personalized digital practices,[170] such as ranking, profiled disclosures, and personalized price, currently lead influential scholars to discuss a somehow provocative,[171] theoretical development for law, namely 'personalized law'.[172]

[168] Montinaro (n 40).

[169] See the news on: <https://en.agcm.it/en/media/press-releases/2007/8/alias-1160> accessed 28 April 2023.

[170] See Quentin, Carmon, Wertenbroch (n 8). The Authors underlined that the phenomenon of 'personalization' «can, on the one hand, contribute to consumer well-being by making consumer choices easier, more practical, and more efficient. On the other hand, they can also undermine consumers' sense of autonomy, the absence of which can be detrimental to consumer well-being. Drawing on diverse perspectives from marketing, economics, philosophy, neuroscience, and psychology, we explore how consumers' sense of autonomy in making choices affects their wellbeing».

[171] Some scholars considered 'personalized law' a provocative idea, because it challenges a central pillar of our legal systems: equality under the law. See Horst Eidenmueller, 'Why Personalized Law?' (2021) U Chi L Rev <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3969934> accessed 20 October 2022.

[172] A seminal article on personalization was written by Ariel Porat, Lior Jacob Strahilevitz, 'Personalizing Default Rules and Disclosure with Big Data' (2014) 112 Mich L Rev 1417. The Authors underlined that personalization could be used to design disclosures tailored to specific individuals to increase the relevance of the information and to reduce the information overload risk. Various areas of law are interesting by personalization process: Christoph Busch, 'The Future of Pre-contractual Information Duties: From

Practically speaking, this (new) perspective has been put forth on both sides of the Atlantic and, as already mentioned in the introduction, it explains how algorithms and Big Data could contribute to shaping the structure and scope of the law based on the study of individual behaviours and attitudes.[173]

In other words, the ongoing trend is based on the 'granular legal norms' idea,[174] which is intuitively the opposite of the traditional law of the State governed by the rule of law, where general and abstract norms ensure the equal treatment of citizens without being under the influence of individual or group interests. A common criticism addressed to the historical western legislative tradition that proceeds for general principles is the risk of unequal treatment.

Using data obtained by artificial intelligence techniques and Big Data analysis, the legislator can tailor legal norms to user cognitive capabilities, personalities and other real features. Consequently, he can strengthen the shift from formal equality to substantial equality. This value is an inherent scope of private law that has characterised this body of law since the 20th century when law had to take account of socio-economic and relational weakness.[175] If standard rules would now leave the floor to personalized rules, there would be different critical issues in comparison to the past.

Currently, the combination of advanced technology and behavioural analysis represents the approach to overcoming the inherent difficulty of the inductive process of abstraction, consisting of inferring a general principle from the analysis of a variety of cases. Granular legal rules can

Behavioural Insights to Big Data', in Christian Twigg-Flesner (ed.), *Research Handbook on EU Consumer and Contract Law* (Elgar 2016) 221-225; Tembot Z. Misostishkhov, *Personalized Law and Fundamental Rights* (2020) 1(4) Digital Law Journal 56-73; Omri Ben-Shahar, Ariel Porat, 'Personalizing Negligence Law' (2016) 91 NYU L Rev 627; Philipp Hacker, 'Personalizing EU Private Law: From Disclosures to Nudges and Mandates' (2017) 25 Eur Rev Private L 651. Among the most proactive professors of law discussing the advantages of personalized law as a new framework for legal research, it is important to refer, in particular, to: Christoph Busch, Alberto De Franceschi, *Algorithmic Regulation and Personalized Law. A Handbook* (Nomos 2021); Alberto De Franceschi, Christoph Busch, 'Granular legal norms: Big Data and the personalization of private law', in Vanessa Mak, Eric T. Tai, Anna Berlee (eds.), *Research handbook on data science and law* (Edward Elgar 2018) 17.

[173] A leading book in the field of personalized law Busch, De Franceschi (n 172) 1. This is why most of the explanations given in this paragraph are indebted to this book.

[174] Busch, De Franceschi (n 172), 408-424.

[175] See Pietro Sirena, 'Personalization in Contract, Consumer and Tort Law ('Granular Legal Norms' in the Financial Services Trade)', in Busch, De Franceschi (n 172) 189.

better respond to specific needs. In this sense, it was noted that 'technology could make it possible to readjust the relationship between individual fairness and legal certainty'.[176]

Considering the attention dedicated in the previous pages to the contribution of other disciplines, such as behavioural economics, it is fitting to describe the brief rebuilding of the debate and main elements of personalized law, starting with its relevance from a comparative law perspective, and its interconnections with other fields of knowledge; the leading critics, and finally what changed in the relationship between law and individuality.

First of all, comparatists noted that the idea of personalized law is not an original one; rather it is rooted in the typical common law case-based method, where norms are tailored to the relationship between parties and their attitudes[177]. Zeno-Zencovich noted that:

'[…] granular norms are (simply?) a return to the past. One destructures a general rule in its thousands, millions of occurrences and applies it casuistically. In this case however the restructuring is not done though a microscopic analysis of precedents, but though digital technologies which, analysing data concerning the parties involved, circumstances, goals (e.g. efficiency) are able to set, *ex ante*, an individualized rule'.[178]

A closer legal analysis shows that granular norms are not absent in European tradition. Unquestionably, the need for 'good governance' of personalized law emerge: to consider technological and behavioural insights into legal interventions, it is important to recognize potential inherent drawbacks. Doubts and criticism relate to the same structural elements of modern personalization, namely technologies and behavioural analysis. Considering a potential bias, not every person acts in the same (biased) way. This is why behavioural elements complicate policies and regulatory standards.[179] What is more, from the perspective of technological insights, algorithmic operations are not 'neutral' as they, ultimately, depend on designers' choices, and consequently they are subject to bias, interests, and human strategic choices.[180]

[176] ibid, 415.

[177] Vincenzo Zeno Zencovich, '"Smart Contracts", "Granular Norms" and Non-Discrimination', in Busch, De Franceschi (n 172) 264-278.

[178] ibid, 275. The Author advised about the limits of such a generalization.

[179] Philipp Hacker, 'The Behavioral Divide. A Critique of the Differential Implementation of Behavioral Law and Economics in the US and the EU' (2015) 1 European Review of Contract Law 327-343.

[180] Mirelle Hildebrandt, Laura Tielemans, 'Data protection by design and technology neutral law' (2013) 29(5) Computer law & Security Review 509-521.

For Casey and Niblett fundamental questions in personalized law concern: (1) source and quality of data, (2) discrimination and bias, (3) human intervention, (4) transparency of data, and (5) regulation of the providers.[181] Essentially, the quality of data a lawmaker relies on, determines the conditions for the algorithm to achieve the objective of the law.

3.4 The drawbacks of personalization: algorithmic discrimination, failures, and meta-preferences impacts

Hypothetically a poor quality of data concerning user behaviour could determine a discriminatory algorithmic operation, and in this sense, granular norms based on algorithmic decision-making can reduce or exacerbate existing biases in the law. Moreover, at least two other critical issues emerge concerning the implied human choices and transparency. Humans are involved in all stages: designing, training, and assessing the operation and aims of the algorithm. Humans could also check from an ex-post perspective if the algorithm result complied with the given ex ante mission. It is still debated under which circumstances a human can 'diverge' from the algorithmic choice and decision, following a path most convincing for him based on knowledge and professional experience. It fundamentally depends on how lawmakers can use algorithms to personalize the law. For decades, algorithms have been an integral component of every computer program. Today, algorithmic decisions dominate many aspects of our lives: beyond the execution of complex computational operations, they, very often, replace the discretion of human choice.

From this perspective, the discussions about the constitutional dimensions of predictive justice are relevant as part of the broader changing landscape at which digital constitutionalism is depicted.[182] In a

[181] Anthony J. Casey, Anthony Niblett, 'A Framework for the new Personalization of Law' (2019) 86(2) The University of Chicago Law Review 349. For the Authors, everything in personalization comes back to objectives. If one propounds the benefits of a personalized law using an algorithm, one must ask whether the algorithm achieves the purpose of law. Frank Pasquale, *The Black Box Society: The Secret Algorithms that control Money and Information* (Harvard University Press 2015).

[182] Among others, on the idea of digital constitutionalism, see Giovanni De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic society* (Cambridge University Press 2022).

controversial 2016 ruling (State or Wisconsin v. Eric L. Loomis),[183] the Wisconsin Supreme Court ruled on the appeal of Mr. Eric L. Loomis, whose six-year prison sentence had been imposed by the Circuit Court. In determining the sentence, the judges relied on the COMPAS (Correctional offender management profiling for alternative sanctions) program, owned by the Northpointe (now Equivant) company, according to which Loomis was identified as a high-risk recidivist. Although it cannot be determinative, a sentencing court may use a Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) risk assessment as a relevant factor for such matters as: (1) diverting low-risk prison-bound offenders to a non-prison alternative; (2) assessing whether an offender can be supervised safely and effectively in the community; and (3) imposing terms and conditions of probation, supervision, and responses to violations. A COMPAS risk assessment may be used to enhance a judge's evaluation, weighing, and application of the other sentencing evidence formulating of an individualized sentencing program appropriate for each defendant.

The appellate court held that using COMPAS risk assessment at sentencing did not violate Loomis' due process right because he failed to show that the sentencing court relied on gender.

The second issue mentioned relates to transparency, a constant concern about algorithms. In AI architectures it is possible to know the inputs and the outputs. Instead, it is difficult to know the ‘reasoning’ of the machine. These digital rationales are not as straightforward as traditional statistical techniques to understand the role played by the different variables in the decision-making process.

Among these theoretical insights, an example of the shift provoked by a personalization legal process would contribute to clarifying the benefits of analysing a legal topic such as consumer autonomy.

In the consumer law field, a relevant evolution of the consumer as a subject showed the need to overcome the European judicial definition of the ‘average consumer’ and move towards the multiplicity of the ‘images of the consumer’.[184] The variety of types of consumers was analysed by the

[183] *State v. Loomis* 881 N.W.2d 749 (2016). The State contends that defendant Loomis was the driver in a drive-by shooting.

[184] The argument is proposed by Sirena (n 175) 187-191. See also Vanessa Mak, The consumer in European regulatory private law, in Dorota Leczykiewicz, Stephen Weatherill (eds), *The images of the consumer in EU law: legislation, free movement and competition law* (Hart Publishing 2016) 381-400.

scholarship that advocates this expression based on different individual consumer behaviours:[185]

> ‘attention was therefore drawn to vulnerable consumers, hasty consumers; consumers with inferior bargaining power; and uninformed consumers. Along a different taxonomy, the following consumer images were to be set out: the fully informed consumer; the information seeker; the passive glancer; the snatcher; the irrational consumer; and the consumer without choices’.[186]

In sum, Big Data and algorithm-based regulation could fundamentally change the design and structure of legal norms: impersonal law based on typification could be replaced by personalized law.

To comprehensively conclude this general description, the potential drawbacks of personalization deserve attention. Are we sure that market automation’s the sort of ‘psychological reductionism’ do not lead to wrong nudges? Are consumer ‘meta-preferences’ taken into account by algorithms? Data-driven marketing mostly focuses on behaviour, at the expense of higher-order psychological processes such as preferences, emotions, and moral judgments: a machine that reveals consumer preferences from Google searches or browsing history on Amazon may ignore mental processes that lead to individual behaviour. This is particularly important in contexts where consumers have aspirational preferences that might differ from those suggested by their past behaviour, namely meta-preferences.

The link between preferences and meta-preferences often reflects the inherent tension between who the person is now and the ideal representation that the individual has of himself and would like to be. By ignoring meta-preferences (which may be inaccessible to the algorithm) and instead focusing on the preferences suggested by past choices, data-driven marketing might deprive consumers of the ability to improve their character and encourage them to repeat choices they wish not to make again.

[185] See Fabian Klinck, Karl Riesenhuber (eds.), ‘§1. Einführung: Das Verbraucherleitbild – Interdisziplinäre und Europäische Perspektiven’, in Fabian Klinck and Karl Riesenhuber (eds.), *Verbraucherleitbilder: Interdisziplinäre und europäische Perspektiven* (de Gruyter 2015); Bastian Schüller, ‘The definition of consumers in EU law’, in James Devenny, Mel Kenny (eds.), *European Consumer Protection: Theory and Practice* (Cambridge University Press 2012) 123; Thomas Wilhelmsson, *Twelve Essays on Consumer Law and Policy* (Department of Private Law, University of Helsinki 1996).

[186] ibid, 191.

4. Research inquiry and method

To sum up, Chapter I mapped the new challenges and opportunities emerging with the advent of data-driven technologies, and it framed them into the current European regulatory and policy framework.

Firstly, the unresolved inadequacy of the sole information approach and the current European legislator's awareness about it come to light. Similarly, legal scholarship sparks discussion on the suitability of complementing the current approach with other policy models and legal tools. With data-driven technologies, the importance of integrating cognitive science insights in regulatory aims is evident, as it has become possible to gain exact knowledge, not only about consumer preferences and cognitive characteristics to profile them but also about consumer misperceptions and vulnerabilities as observed in real-time.

The proposal for a tight integration between behavioural insights and regulation is even more crucial if taking into account the fact that regulatory models and legal prototypes applicable to data-driven technologies are still widely debated. In contrast, in the meantime, information technology evolves and the cost of data collection, storage, and processing declines. Analysing large volumes of unstructured data (Big Data) could play a transformative role for models to protect consumer autonomy.

Critical issues derived from data-driven scales, predictive power, and also from the fact rationales are numerous and still insufficiently explored: the statistical source they are based on, for example, can not recognize the consumer meta-preferences variables which could, case by case, be crucial to turn the consumer's mind toward the opposite choice than the algorithmically predicted one. Thus, people might not defer choices relevant to their identity to such algorithms.

The forward-looking perspective proposes rooting regulation on behaviourally personalized information, instead of standardized (impersonal) information, to increase adequate protection of autonomy.[187] Building a personalized legal approach using data and algorithms is on our

[187] Scholarship on effective information design should be taken into exam: Ognyan Seizov, Alexander J. Wulf, Joasia Luzak, 'The Transparent Trap: A Multidisciplinary Perspective on the Design of Transparent Online Disclosures in the EU' (2019) 42 J Consumer POL'y 149.

doorstep.[188] Should we welcome this transformation of law as a techno-regulation tool that strengthens consumer autonomy? How can digital design or digital architecture contribute to enforcing fair and lawful data processes and consumer protection?

The investigation will be conducted in the following pages by analysing the consumer (cognitive) vulnerabilities related to digital architecture and designs. The case-study of dark patterns will exemplify how quick and easy it can be to scrap user consent with malicious intent, and obtain consumer responses formally compliant with the current EU legal framework, but substantially not authentic, and consequently deviating from genuine autonomy.

Within the evolving legal and technological setting described (see section 3), the research inquiry aims to investigate the tension between the formal current European legal protection of the multidimensional concept of autonomy and its concrete efficacy, through the case of dark patterns. For the intricate frame of applicable provisions, the analysis will consider the main rules of consumer law, data protection law and competition law to understand the extent to which the frame is still effective, and to which traditional notions require a new interpretation.

The research inquiry, furthermore, engages with the practical role the architectural digital design can play in avoiding pitfalls in the efficacy of current legal framework, and in constructing effective protection of consumer autonomy.

Implied sub-objectives will contribute to analyse the effectiveness and robustness of the complex and overlapping legal framework currently protecting consumer choices under the effect of dark patterns.

From a methodological point of view, the ambitious and articulated goal requires the adoption of a perspective able to consider a multidisciplinary and empirical approach, which informs EU policymaking regarding the design of digital architectures. To realize this aim, the analysis must profit from the advances provided by a Law 3.0 scenario, as a starting point for integrating normative and non-normative tools.

[188] Following the perspective of a personally tailored law, the 'reasonable person' standards would be replaced by a multitude of personalized commands (skilled doctors would be held to higher standards of care; age restrictions for driving would vary according to recklessness risk that each person poses, and so on).

II

WHEN AUTONOMY STRUGGLES WITH *DARK PATTERNS*: PROMISES AND PITFALLS OF THE CURRENT EU REGULATORY PATCHWORK

1. Perspective and approach of the Chapter

The previous chapter has recognized the structural directions taken to counter the risks to consumer autonomy posed by fast-moving data-driven technologies.

Based on these premises, the current chapter moves forward, considering that risks to user autonomy no longer come only from the quantity of information and transparency but also, and predominantly, from factors like tricky digital structures. Consequently, the issue of controlling choice architecture, meaning how to assess fairness, becomes crucial.

Thus, the perspective toward the protection of autonomy becomes slightly different: instead of focusing on the remedies for the injured consumer offered by European law, the analysis centres on the nature and origins of threats, namely dark patterns, recognizing which provisions ensure fair and lawful choice architectures.

To sum up, the research moves the focus from transparency to fairness because autonomy protection in the digital environment develops towards a twofold core: information duties and a fair design. Relate issues on how a designed interface could be a human-centred design, respectful of consumer free choice led to investigating the requirements digital interfaces must meet: a critical issue questions if current regulations and judicial interpretation can be sufficient to redesign adequate information disclosures or more generally, to protect consumers from potential exploitation of their cognitive bias.

Specific attention will be dedicated to the efficacy of those existing principles and legal tools, such as free consent, guaranteeing that digital architecture is legally compliant both formally and substantially. In marketing law and data protection law, consent constitutes an integral part of empowerment, for example.

Equivalent attention will be given to the analysis of fairness, a concept which is generally referred to as human behaviour, which nowadays also becomes a pivotal principle of AI ethics, which models algorithmic operations to democratic values, such as freedom and equality.[1]

Put simply, the concept of unfairness, developed in consumer law, cannot be ignored when assessing data exploitation strategies under the GDPR. Indeed, GDPR must be perceived as an essential pillar of consumer protection law, even because it is, in itself, a sort of due diligence process: data controller must ensure legitimacy, transparency and security, respecting the principle of proportionality, demonstrating accountability and ensuring empowerment of data subject.

Given this relevance, the design architecture will be investigated as a meaningful path toward an effective response to the protection of data-subject/consumer autonomy.

The regulatory fields considered will comprise two main areas of private law, tightly connected and complementary to each other: data protection law and consumer law. Moreover, key interconnected elements of another field of law – competition law – will also be considered, even if mostly in general terms, on the assumption that unfair digital design could also be anticompetitive, and consequently impacts consumer options.

Notwithstanding their different rationales – fair processing for data protection law and fair transactions for consumer law – this Chapter explores the implicit potentialities for a more holistic vision of data consumer law.[2]

From a structural point of view, the impact of dark patterns on the several mentioned policies will be emphasized, together with their interconnection and their efficacy for substantial autonomy protection. Additionally, suitable amendments will be proposed to provide the basis for further discussion in Chapter III.

[1] Franziska Koefer, Ivo Lemken, Jan Pauls, 'Fairness in algorithmic decision systems: a microfinance perspective' (2023) 88 EIF Research and Market Analysis Working Paper. For scholars, a situation is considered fair, if all reasonable and equal persons agree to it. John Chapman, 'Rawls's theory of justice' (1975) 69(2) The American Political Science Review 588-593.

[2] Helberger *et al.* (n 159 Ch. I) 1427.

2. Design patterns and the pervasive phenomenon of dark patterns

As anticipated in Chapter I (section 2.3), a slightly different phenomenon from nudging nowadays worries legislators in Europe, and many other countries: dark patterns which exploit bias to exclusively pursue the operator interest to the detriment of user interests, or public interests. Very often what seems to configure a poorly designed web-interface is the result of choices specifically made to misuse user cognitive bias, increasing the providers' profit.[3] This malicious aim does not fit a digital design that is genuinely required to give priority to the protection of fundamental rights, including the right of self-determination. The result will be a design pattern which will not ensure substantial transparency, fairness, and compliance with ethical and normative principles.

Indeed, the choice of digital architecture affects the presentation and quality of information to the user and, consequently, their decisions.

Manipulative designs induce users to perform certain actions unconsciously.[4]

Harry Brignull[5] originally aimed the term dark patterns. Recently, the efforts of legal research and European regulatory documents focused on identifying and classifying the polyhydric practices included under the label of dark patterns.

Looking firstly at the academic contributions dedicated to the topic,[6] dark patterns are commonly identified as 'user interface design choices that

[3] About cognitive bias: Amos Tversky, Daniel Kahneman, 'Judgment under Uncertainty: Heuristics and Biases' 185 (4157) Science 1124-1131.

[4] For reading on how architecture can guide user behaviour: Karen Yeung, "Hypernudge": Big Data as a mode of regulation by design' (2017) 20(1) Information, Communication & Society 118-136.

[5] Harry Brignull is an expert in User Experience Design (or UX design). He has documented dark patterns for more than 10 years. Thus, studies of cognitive science and the habits of human behaviour are used in the creation of dark patterns to bring exclusive benefits to the company rendering the service, such as a temporary increase in revenue or an increase in subscribers or, for that matter here, a collection of personal data for which the user would be unlikely to have given informed consent. All the information could be found on Harry Brignull, *Deceptive Patterns. Exposing the Tricks Tech Companies Use to Control You* (Testimonium Ltd 2023). In 2010 Brignull identified 12 types of dark patterns. By 2021, the number of dark patterns variants had increased to about 27.

[6] Generally observing, besides the first taxonomy of dark patterns proposed by Harry Brignull, academic proposals are numerous. As Mark R. Leiser, Wen-Ting Yang, 'Illuminating manipulative design: From 'dark patterns' to information asymmetry and the repression of free choice under the Unfair Commercial Practices Directive' (2022) note No. 8 SocArXiv. Examples of taxonomy (in part overlapping with the Brignull's

benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions'.[7] Behavioural economists prefer to consider dark patterns as species of sludge[8], while other academic researchers consider them a type of market manipulation.[9]

The idea is not new. Firstly, it harks back to unfair commercial practices (see below in section 5.2). However, due to the global dimension of e-commerce, dark patterns are even more sophisticated, dangerous and widespread in the digital environment than the well-known unfair practices. Dark patterns appear not only in cookie banners: they are also prevalent, with variations, in social media settings, e-commerce, and fitness apps that users install on their mobile devices. They proliferate in chatbots and virtual assistants whose mission is to learn about their users and generate knowledge to persuade and proactively engage in triggering – or even originating – (new) vulnerabilities.

These practices impact on consumers in a variety of ways: they can mislead them, distort their choices and behaviour, or make certain decisions more prominent, more difficult, or more accessible. Dark patterns can create a false feeling of urgency, or a 'missing out' fear (e.g., the use of a 'high demand' message), or a feeling of guilt via social

original classification are: Gregory Conti, Edward Sobiesk, 'Malicious Interface Design: Exploiting the User' (Proceedings of the 19th International Conference on World Wide Web 271, 2010), 272-273 at <https://doi.org/10.1145/1772690.1772719> accessed 27 September 2021; Colin Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, Austin Toombs, 'The Dark (Patterns) Side of UX Design' (Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Article no. 534, 2018); Arunesh Mathur, Gunes Acar, Michael Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, Arvind Narayanan, 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 Proceedings of the ACM on Human Computer Interaction 81, 82; Şebnem Özdemir, 'Digital nudges and dark patterns: The angels and the archfiends of digital communication' (2020) 35 Digital Scholarship in the Humanities 417; Giuseppe Versaci, 'Consenso al trattamento dei dati personali e dark patterns tra opzionalità e condizionalità' (2022) 5 NLCC 1130; Midas Nouwens, Ilaria Licciardi, Michael Veale, David Karger, Lalana Kagal, 'Dark Patterns after GDPR: Scraping consent pop-up and Demonstrating their Influence' (2020) 1-13.

[7] Shruthi Sai, Chris Watkins, Lucca McKay, Colin M. Gray, 'Nothing Comes Before Profit': Asshole Design In the Wild' (2019) CHI Conference on Human Factors in Computing Systems 1-6.

[8] Cass Sustain, 'Sludge and Ordeals' (2019) 68 Duke L J 1843-1883; and Richard H. Thaler, 'Nudge, Not Sludge' (2018) 361(6401) Science 431.

[9] Ryan Calo, 'Digital Market Manipulation' (2014) 82 Geo Wash L Rev 995-1051; and Jon D., Hanson, Douglas A. Kysar, 'Taking Behavioralism Seriously: The Problem of Market Manipulation' (1999) 74 NYU L Rev 632-749.

influence or peer pressure, or they can obstruct or confuse consumers, also by sneaking items into the shopping basket. Every specific form of dark patterns, and consequently their legal assessment, depending on how and to what purpose they are used (e.g. 'pre-formulated declarations of consent', 'clickwrap contract' and 'cookies walls' specifically aim at scraping consent).

Within such a diverse scenario, Luguri and Strahilevitz observed that a first wave of research seeks to create a helpful taxonomy of dark patterns, while a second wave of scholars established the growing prevalence of these techniques.[10] The overall goal of numerous taxonomies is to understand better the legal challenges behind dark patterns, mainly how designers affect the data-subject decision-making process.[11]

For the scope of this book, it is not necessary to present the fully extent of categorization proposed by academics. I will limit the description of dark patterns to the sole official document that disciplines the phenomenon.[12]

The European Authorities[13] have recently published a commonly accepted taxonomy of DP. Specifically, the reference model is based on content and type of interface: the attempt was carried out by the European Data Protection Board (Edpb) based on Article 60 of the GDPR. The

[10] Jamie Luguri, Lior Strahilevitz, 'Shining a Light on Dark Patterns' (2021) 13(1) Journal of Legal Analysis 43. The Authors advanced in this field of research, proposing to answer a question dealing with the effectiveness of dark patterns.

[11] Luiza Jarovsky, 'Dark Patterns in Personal Data Collection: Definition, Taxonomy and Lawfulness' (March 1, 2022), available at:
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4048582> accessed 10 June 2022.

[12] The continued use of the term 'dark patterns' could provoke a growing discordance between legal experts and the HCI multidisciplinary community. (Mis)using of the term 'dark pattern' to attack a practice that appears manipulative is standard. This phenomenon hinders effective regulation. See Leiser, Yang (n 6).

[13] Concerns about the diffusion of dark patterns also exist in other countries, as US and Southeast Asian e-commerce. A digital media company, for example, reporting on the most promising technology-driven businesses and trends in the world's emerging markets, revealed the prevalence of dark pattern-inspired user design in Southeast Asian e-commerce. Almost every e-commerce site in the region – including Lazada, Bukalapak, Sendo, Tokopedia – bombards visitors with a dense interface, aiming for information saturation on smaller mobile screens. Consumers are flooded with kaleidoscopic mixes of coupons and item listings, many tagged with nominal sale prices. Sites also foment a false sense of urgency in anyone who may just be browsing, using hourly 'flash sales' coupled with low-stock notifications to capitalise on scarcity bias and encourage users to add items to their basket – putting them one step closer to a transaction. Now available a <https://kr-asia.com/>.

Board published the Guidelines 3/2022 dedicated to Dark patterns in social media platform interfaces: how to recognise and avoid them,[14] a soft law document addressed to designers to avoid the insertion of dark patters within sites, social platforms, and consent management platforms (CMPs) in websites to manage user privacy consent.[15]

A short description, as follows, of the main characteristics of every category proposed by the EDPB will be helpful to understanding the type of exploitation.

Overloading, based on which users are confronted with a large amount of information, requests or options to prompt them to share more data, or unintentionally allow personal data processing against the data subject's expectations.

This first category includes three specific types of patterns: *continuous prompting; privacy maze; and too many options.* Continuous prompting is the practice of re-proposing at each access the same request for information that the user initially refused to grant. As a result, the user will be inclined to give the requested information to not see the request reappearing again.

The so-called content-based privacy maze occurs when data protection information, instead of being placed in the same place, is in different tabs, resulting in inconvenience to the user. Such a situation can occur when the privacy notice is structured to make it more difficult for the user to read and understand the information contained within it.[16]

[14] European Data Protection Board (Edpb) 'Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognize and avoid them' (version 1.0), adopted on March 14 2022.

[15] Cristine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, Thorsten Holz, '(Un)Informed Consent: Studying GDPR Consent Notices in the Field' (2019) Proceedings (ACM SIGSAC Conference on Computer and Communications Security) <http://dx.doi.org/10.1145/3319535.3354212> accessed January 10 2023. In this recent study, about 1,000 CMPs (Consent management platforms) were analysed: at least 57.4% of them used dark patterns to push users to adopt less privacy-friendly options. Then, 95.8 percent of these either provided no choice regarding consent on processing of one's personal data, or only provided the option of accepting the processing and 'adjusting' it to the user's actual wishes. The cited study also showed that the acceptance rate of privacy options rises from 0.16% to 83.55% they are already pre-selected by the service provider.

[16] A Norwegian study showed how dark patterns are used to 'push' users toward more privacy intrusive option. The study is conducted by Forbrukerrädet, an organization that protects consumer interests and was founded by the Norwegian government. Part of its work promotes consumer rights, such as the right to privacy and the right to secure and balance contracts when purchasing digital products or services. The study cited above includes among the elements that manipulate users into giving up their data under the illusion of control, the use of default settings, the use of misleading words, and the choice

With the *too-many options pattern,* the number of choices leaves users unable to make any choice or makes them overlook some settings, especially if information is unavailable. It can lead them to finally give up or miss the settings of their data protection preferences.

The *skipping* pattern class induces the user to forget or not think about all or some data protection aspects. The so-called *deceptive snugness* and the *look over* are subcategories. The former is exclusively related to the interface. An example is intrusive data features and options enabled by default: this constitutes a dark pattern because, usually, the user keeps the pre-selected options without evaluating the others available.

The second the *look over there* is an interface used to distract the user's attention towards elements that are unrelated to data protection. To exemplify, the controller reports through texts that contain a lot of non-relevant information and omits the relevant details.

The category of *stirring* patterns affects user's choices by appealing to their emotions or using visual nudges. Subcategories are *emotional steering* and *hidden in plain sight* patterns. In the former, emotional steering, wordings or visuals are used in a way that conveys information to users in either a highly positive manner, making users feel good or safe, or a highly negative one, making users feel anxious or guilty.[17] The latter, *visual options* use a visual style for information or data controls that nudge users away from advantageous data protection options towards less restrictive and thus more invasive options.

The *hinderingpatterns* hinder users in various ways, such as obstructing or blocking users becoming informed or managing their data by making the action difficult or impossible to achieve. Its subcategories are *dead ends, longer than necessary, and misleading information.* In the first case, some links that

of 'architectures' of websites that require the user to put more effort into taking measures to protect their personal data, thus discouraging them from taking such actions. Norway Forbrukerr˚adet, *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Forbrukerr˚adet, Norway, 2018, available at: <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

[17] It is interesting to note since the very beginning that influencing decisions by providing biased information to individuals can generally be considered an unfair practice, contrary to the principle of fairness of processing set in Article 5 (1) (a) GDPR. It can occur throughout the entire user experience within a social media platform. However, the stirring effect can be especially strong, at the sign-up process stage, considering the overload of information that users might have to deal with in addition to the steps needed to complete the registration. European Data Protection Board (n 14) 17.

would allow the user to exercise his or her rights are missing, or the interfaces appear to be unresponsive to commands; in the second case, the unnecessary prolongation of the choice process is questioned, or the proliferation of opt-out versus opt-in steps are characterised the interface; and in the third, misleading information is used, which makes the user believe that the information to be provided is indispensable to obtain a result. In this case, the dark pattern violates the principle of minimisation, which requires that only data strictly necessary to achieve the purposes be collected and processed.

Fickle patterns generate an unclear design: the interface is inconsistent and makes it difficult for the user to navigate through the data protection control tools and understand the purpose of processing.

Lacking hierarchy and *decontextualising* are subcategories. The first case occurs when the information given to the user is not divided into sections or paragraphs, making it difficult to read it, or in cases where a social platform differs a little from the usual design model: this occurs when in different device versions of a social platform the settings are displayed with a different symbol. The second case, so-called *decontextualizing* occurs when an information or data protection control option is located on a page out of context and becomes difficult for the user to find because it has a non-intuitive location.

With the *left in the dark pattern*, uncertainty prevails as the interface is designed to hide information or data protection control tools, or to leave users unsure of how their data is processed and what kind of control they might have over it regarding the exercise of their rights. Language discontinuity, conflicting information or ambiguous wording are subcategories. *Language discontinuity* occurs when information about data protection is not provided in the official languages of the country where users live, as opposed to the service. *Conflicting information* leaves the user uncertain about what they should do and the consequences of their actions: for example, the social network informs the user of control over their sharing preferences but at the same time specifies that it is not possible to change them on content posted.

Finally, the use of *ambiguous words* or information is also *dark*: for example, using conditional or vague wording that leaves the user uncertain about the use of the data and the purpose of the collection; or using specific or technical language that is difficult for the average user to understand.

It is clear from this brief overview that the variety and diversity of circumstances have configured problems, primarily at the crossroad between data protection and consumer law.[18]

From an ethical point of view, user concerns also increase as data collectors have the tools to manipulate individual information.[19] Knowing or inferring a person's preferences allows one to exert considerable influence over that person; it is possible to find out their goals, their weaknesses, and vulnerabilities, and when and how they are influenced.

2.1 Dark patterns and consumer harms. The threats to self-determination data and consumption choices

Potential material and non-material harms caused by dark patterns could be various: they could be economic, such as the payment of a higher price or an unwanted subscription to service; they could be privacy harms, such as the disclosure of more personal information than necessary, or by giving consent to invasive privacy practices; they could cause emotional or psychological distress, such as the feeling of guilty about a particular choice, feeling cheated, fear of missing out, emotional pressure; or the wasting of time, for example, trying to avoid being tricked, or choosing the 'unpreferred' path in order to select privacy protective settings.[20]

[18] On the application of the Unfair Commercial Terms Directive to dark patterns see the recent recommendations of the European Consumer Organization: 'Dark Patterns' and The Eu Consumer Law Acquis. Recommendations for better enforcement and reform', 2022 <https://www.beuc.eu/publications/beuc-x-2022-013_dark_patters_paper.pdf> accessed 10 December 2022. The document states: the use of unfair practices to distort consumers' economic behaviour is not new, but it takes a new important dimension as a result of the massive collection of data and the use of technology to build consumer profiles and anticipate consumer behaviour. EU consumer law already has partial capacity to address these situations, but it is currently not sufficiently enforced. In addition, EU law must be updated to tackle these unfair practices and ensure consumers are not harmed by misleading user interfaces and data personalization techniques (at 1).

[19] Cfr. Daniel Susser, Beate Roessler, Helen Nissenbaum, 'Technology, autonomy, and manipulation' (2019) 8(2) Internet Policy Review <https://doi.org/10.14763/2019.2.1410> accessed 23 August 2022.

[20] The harms were identified by David Martin, *Dark patterns: impact on consumers and potential harm*, during the IMCO Public Hearing 'Dark Patterns and How such Practices Harm Consumers and the Digital Single Market' – meeting 16 March 2022. This presentation is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020), available at <https://www.europarl.europa.eu/cmsdata/246802/BEUC%20PPT%20Dark%20Patterns%20Hearing%20IMCO-16%20March%202022.pdf> accessed 8 May 2023.

All the different harms have the exact origin: a material distortion of consumer choice and behaviour. Indeed, many threats originate from the exploitation of cognitive bias, which confirm the importance of analysing the concept of digital vulnerability (see Chapter III).

First, dark patterns manipulate consumers by altering online choice architecture in ways designed to thwart user preferences for objectionable ends. They make it possible but asymmetrically tricky for a user to act in a manner consistent with their preferences 'often by prompting impulsive System 1 decision-making and discouraging deliberative System 2 decision-making'.[21]

In other words, all the mentioned harms violate individual self-determination: considering this concept in a broad sense, self-determination nowadays is not only related to the governance of data, but it is also extended to consumers' choices of consumption.[22]

Western legal traditions focus on the protection of fundamental rights, and there is a conspicuous case law over time, interpreting the right of individual autonomy, or self-determination, firstly in the traditional offline environment,[23] and then concerning to information self-determination.[24]

The specific dimension of informational autonomy has been interpreted as a related meaning of self-determination, which in turn was treated by the courts as a concept derived by the right to privacy:[25] the capacity to choose (see Chapter I). The several variants of case law determined for analysing autonomy as self-determination represent the

[21] Kahneman (n 85 Ch. I).

[22] See Leonard Lee, On Amir, Dan Ariely, 'In Search of Homo Economicus: Preference Consistency, Emotions, and Cognition' (2006), available at: <https://ssrn.com/abstract=925978> accessed 13 January 2023.

[23] For example, the field of medical malpractices demonstrated that, in critical circumstances, balancing judgment of the fundamental rights means to ultimately protect the right to free self-determination of the person's giving consent. For an overview see Giorgia Guerra, 'Lo «spazio risarcitorio» per violazione del solo diritto all'autodeterminazione del paziente Note a margine di un percorso giurisprudenziale' (2010) II (12) Nuova giur civ comm 617-632.

[24] See Cécile De Terwangne, *The Right to be Forgotten and the Informational Autonomy in the Digital Environment* (Publications Office of the European Union, 2013 the report was written for the European Commission, 2013, Report EUR 26434 EN).

[25] The recognition of a right to personal autonomy as enshrined into the right to respect private life protected by article 8 ECHR, see ECtHR, Evans v. United-Kingdom, 7 March 2006, req. n° 6339/05; and in ECtHR, *Tysiac v. Poland*, 20 March 2007, req. n° 5410/03; ECtHR, *Daroczy v. Hongary*, 1 July 2008, req. n° 44378/05.

free development of personality and interpersonal relations, as well as the free participation in society.

One of the correlations of autonomy with the protection of self-determination resulted from the regulation of the consumer's transactional decision-making under Art. 2 (k) UCPD. This is an actual feature the UCPD holds for consumers in digital markets who will often lack access to relevant data about the audience selection of advertisements and alternative ads they could have seen instead.

In Trento Sviluppo,[26] the ECJ stated that the concept of a transactional decision is broadly defined, as it 'covers not only the decision whether or not to purchase a product, but also the decision directly related to that decision, in particular the decision to enter the shop'.[27] It is important to note that the formulation 'causes or is likely to cause' does not require proof of an actual distortion of the consumer decision-making. A merely hypothetical consideration of the likelihood of a distortion is enough to pass the threshold.

Risks associated with persuasion attempts increase because online platforms combine extensive use of personal data with interfaces designed to shape choice architecture. According to several scholars, online platforms are applying different forms of user surveillance and manipulation.[28] Information asymmetry between consumers and traders is, as always, a typical *fil rouge,* as it refers to the fact that traders hold more information than consumers regarding the product: hiding information, delay in providing information, or providing wrong information are all possible causes of information asymmetry. A slightly different concept of asymmetry characterised the feature in the digital environment where it becomes a structural feature, which will be discussed further in Chapter III.

Making informed decisions requires having control over personal information (e.g. sensitive data, biometric data). This means the individual's right to determine which information about themselves will be disclosed, to whom and for which purpose.

[26] Case C-281/12 *Trento Sviluppo srl, Centrale Adriatica Soc. coop. arl v. Autorità Garante della Concorrenza e del Mercato* EU:C:2013:859, para 36.

[27] ibid

[28] See the scholars on market surveillance regulation: e.g. Christoph Busch, 'Rethinking Product Liability Rules for Online Marketplaces: A Comparative Perspective (Consumer Law Scholars Conference in Boston' (March 4-5, 2021), <https://ssrn.com/abstract=3784466> or <http://dx.doi.org/10.2139/ssrn.3784466> accessed 20 July 2022.

The idea of informational self-determination, first introduced by the German Constitutional Court,[29] latter entered the European level through the right to personal data. The European Court of Human Rights has derived this new dimension of privacy from Article 8 ECHR.[30] Since 1981, the Council of Europe (Convention 108) has established protection regarding the automated processing of personal data.[31]

The European Union Charter of Fundamental Rights is the first general international catalogue of fundamental freedoms and rights that has mentioned the right to data protection as an autonomous right, protected as such.[32]

In cases of harm to the consumer informational autonomy right, European jurisprudence conveys well-established positions regarding the nature of the data-subject consent on the disposal of his or her data. Judges adopted, as well as recent lines of interpretation that address the most innovative profiles on the subject, to protect the user's self-determination and who is the victim of dark pattern mechanisms, or web scraping.

Nevertheless, the impacts of dark patterns on consumer autonomy are, as already emerged in Chapter 1, slightly different: data-driven business practices are increasingly used to develop more effective artificial solicitations to attract consumer attention and influence them, defined as a manipulative form of *hypernudging*.[33] It results in the impairment of user autonomy since it undermines both the authenticity of information and the ability to make decisions by interfering with it. In the following pages this is why it will be important to individualise the legislative coordinates already in act to protect digital consumer autonomy in such circumstances, meaning when choice architectures lead to a consumer behaviour modification. Moreover, due to the nature of potential harms for dark

[29] BundesVerfassungsGericht (n 22 Ch I).

[30] See, among others, E.Ct.H.R., Rotaru v. Romania, 4 May 2000, appl. no 28341/95, § 43; Amann v. Switzerland, 16 February 2000.

[31] Council of Europe Convention 108 for the protection of individuals with regard to the processing of personal data (ETS No 108, 28.1.1981) <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf> accessed 12 June 2023.

[32] Council of Europe Charter of Fundamental Rights of the European Union, [2016] OJ L C-364/1. Article 8.1 states: «Everyone has the right to the protection of personal data concerning him or her».

[33] Cfr. Karen Yeung, 'Hypernudge': Big Data as a mode of regulation by design' (2006) 20(1) Information Communication and Society 1-19.

patterns, a debated issue in case law will concern non-material damages. The question for companies will be whether a breach of the GDPR in the processing of customer data, and to the known risk of a claim for injunctive relief also give rise to a claim for non-material damage under Article 82 GDPR. In other words, if in case of any confirmed infringement of GDPR provisions, in addition to the known risk of a claim for injunctive relief, the injured party considers if the circumstances also give rise to a claim for non-material damage under Art. 82(1) GDPR, for which the claimant must determine the threshold of seriousness. A recent ECJ decision stated that the requirement of a certain degree of seriousness of non-material damage caused to the data subject is not compatible with Art. 82 GDPR.[34]

Regulation in force already presents key elements that controllers and processors must consider when implementing data protection by design, concerning to social media platforms.

Based on the Edpb's Guidelines 4/2019 on article 25 Data Protection by Design and by Default,[35] for example, regarding the principle of fairness, the data processing options should be provided objectively and neutrally, avoiding any deceptive or manipulative language or design.

The Guidelines 4/2019 also identify elements to meet the Data Protection by Default and Data Protection by Design, which becomes concretely relevant for the protection against dark patterns: it states that data subjects should be granted the highest degree of autonomy possible to determine the use made of their data, as well as autonomy over the scope and conditions of that use or processing. Power balance should be a vital

[34] Case C-300/21 *UI v Österreichische Post AG.* [2023] EU:C:2023:370. The ECJ also clarifies that data subject is exempted from demonstrating that a breach of the GDPR has caused any emotional damage at all. The mere infringement of the provisions of the GDPR is, therefore, not sufficient to justify a claim for damages. As far as the amount of a possible claim for damages is concerned, however, the ECJ remains vague: although, according to the ECJ, it is in principle up to the individual legal systems within the EU Member States to make statements on the amount of damages, the national court called upon to make a decision must ensure that the financial compensation also fully compensates for the concrete damage suffered, without, however, constituting a kind of punitive damages.

[35] European Data Protection Board (Edpb), Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020 (The version 1.0 was adopted on 13 November 2019, <https://edpb.europa.eu/edpb_it> accessed 9 January 2023.

objective of the controller-data subject relationship. If it is impossible to avoid power imbalances, data controllers should recognize and account for suitable countermeasures. Data processing information and options should be provided objectively and neutrally, avoiding any deceptive or manipulative language or design. The controllers must provide available information about how they process personal data.

They should not 'lock in' their users in an unfair manner. Whenever a service processing personal data is proprietary, it might create a lock-in to the service, which might not be fair if it impairs the data subject's ability to exercise their right of data portability by Article 20 GDPR.

To enter the lively discussion, the following pages will first outline the essential references in European law to grant authentic consumer protection against deceiving designs.

3. A preliminary 'map' of the European regulatory framework coping with dark patterns

The analysis of the criticalities impacting on consumer autonomy, under the pressure of dark patterns, implies the ability to individualize the frame of European regulations concurring to protect consumers from deceiving digital architectures. Complicating the 'scene' is the contributory factor of the control of digital architecture being realized considering two layers: the standard-formal requisites and the concrete-specific circumstances.

An interplay of different potentially applicable policies emerges: the reference provisions belonging predominantly to consumer protection, data protection and competition law.[36]

The analysis of this interplay between these areas of EU private law is not a new feature: it started in 2014 when the European Data Protection

[36] Mark R. Leiser, 'Chapter 10: Dark patterns: The case for regulatory pluralism between the European Union consumer and data protection regimes', in Eleni Kosta, Ronald Leenes, Irene Kamara (eds), *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022) 240-269; Philipp Hacker, 'Manipulation by Algorithms. Exploring the Triangle of Unfair Commercial Practice, Data Protection, and Privacy Law' (2021) European Law Journal 1; Mark R. Leiser, Mirelle M. Caruana, 'Dark Patterns: Light to be Found in Europe's Consumer Protection Regime' (2021) 10(6) European Consumer and Market Journal 237-251.

Supervisor proposed it as a topic of debate.[37] A very proactive role was played by different Authorities even with soft law instruments. From this perspective, the roles played by the European Consumer Organization (BEUC),[38] and the European Data Protection Board (Edpb) must be emphasized.

Considering soft law documents on dark patterns and the EU Consumer Law Aquis,[39] the BEUC recommends the need to strengthen the protection offered by Directive 2005/29/EC on unfair commercial practices,[40] together with Directive 2011/83/EU on consumer rights,[41] and Directive 93/13/EEC on unfair terms in consumer contracts,[42] and subsequent amendments occurring within Directive (EU) 2019/2161.[43] In

[37] EDPS, 'Privacy and competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the Digital Economy' (2014) <https://edps.europa.eu/sites/edp/files/publication/14-03 26_competitition_law_big_data_en.pdf> accessed 7 November 2022.

[38] The Bureau Européen des Unions De Consommateurs (BEUC) is a European organization that brings together various consumer protection associations and thus represents a considerable audience of stakeholders. The bureau constantly monitors regulatory and case law developments.

[39] Bureau Européen des Unions de Consommateurs (BEUC), 'Dark Patterns' and the EU Consumer Law Aquis. Recommendations for better enforcement and reform' [2022] available at: <https://www.beuc.eu/publications/dark-patterns-and-eu-consumer-law-acquis/html> accessed 15 May 2023. Moreover, the 'Study EU Consumer Protection 2.0 – Structural asymmetries in digital consumer markets' [2021] published by BEUC considers users' digital vulnerability, consent management, informational asymmetry and personalized prices. The document, in particular, offers a careful and in-depth analysis of the penalizing practices of consumers/interested parties, as well as the regulations that can currently be employed to protect them.

[40] Parliament, Council Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), in [2005] OJ L 149 22-39.

[41] Parliament, Council Directive 2011/83/EU 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 Text with EEA relevance [2011] OJ L 304, 64-88.

[42] Directive 2011/83/UE (n 41).

[43] Parliament, Council Directive (EU) 2019/2161 of the 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernization of Union consumer protection rules, [2019] OJ L 328, 7-28.

April 2022, the EU Innovation Council and SMEs Executive Agency, under the mandate of the European Commission, published the report 'Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization', observing the general lack of awareness about the unfairness of many online practices.[44] The legal assessment conducted for this study shows that the regulation of unfair commercial practices in the digital environment allows the intersection of consumer protection, data protection, and other relevant EU policies, including new and future legislation such as the Digital Services Act, the Digital Markets Act, the AI Act, and the Data Act. This would happen every time data exploitation was considered an unfair commercial practice.

Lastly, with dark tactics, tech firms can exclude competition the digital markets and extract the necessary resources akin to restricting in product market.[45]

As noted earlier by the European Commission,[46] dark patterns are manipulative means of distorting privacy, and controlling the processing of personal data. Dark patterns 'materialized' a design lacking due transparency and a poor-quality message. What counts is the technological infrastructure developed and installed before contacting the consumer. Although it is a crucial aspect, the amendments to the UCPD, introduced by Article 2 m) and n) of the Directive (EU) 2019/2161 and referring to rankings and online marketplaces, do not explicitly mention technological infrastructure.

[44] Council, SMEs Executive Agency (EISMEA), 'Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization' (Publications Office of the European Union 2022).

[45] See Greg Day, Abbey Stemler, 'Are Dark Patterns Anticompetitive?' (2019) 72(1) Alabama Law Review <https://ssrn.com/abstract=3468321 or http://dx.doi.org/10.2139/ssrn.3468321> accessed 10 October 2022. The Authors argue that digital manipulation should, in many instances, be anticompetitive. The problem is that antitrust has typically viewed efforts to coax, or persuade, consumers as forms of competition, or even procompetitive behaviour. We show that digital manipulation erodes users' ability to act rationally, which empowers platforms to extract wealth and build market power without doing so on the merits. In fact, as antitrust enforcers and scholars begin to characterize conventional privacy as a benefit of competition, our research asserts that antitrust enforcement should go further in promoting decisional privacy. This would not only increase consumer welfare and generate competition in digital markets, but also fill pressing gaps in consumer protection laws.

[46] Commission, 'Communication to the European Parliament, the Council and the European Economic and Social Committee. 'A New Deal for Consumers' COM/2018/0183 final.

The principle of data process transparency is, first of all, disciplined by European data protection law, and then – for some scholars – it is also a legitimate factor of an 'assisted informed consent' widespread in consumer law.[47]

Taking the perspective of data protection law, it requires technology to be designed in such a way that privacy is protected. In fact, 'empowerment in data protection law does not mean that data subjects have absolute control over what data are being processed about them, nor by whom. The processing of personal data must be 'lawful', which must require that the activity also comply with the UCPD'.[48]

This is also why authoritative scholars have emphasized that privacy code should be embedded in the infrastructure itself.[49]

Stating that 'the processing of personal data should be designed to serve mankind', recital 4 of the GDPR suggests that 'privacy-by-design' (PbD) should be understood as a broad, overarching concept of technological measures for ensuring privacy through an adequate enforcement (see section 3.3). The European legislator indicates that technology producers, as well as designers are responsible for evaluating potential risks to data in the use of their service, as they are considered in the best position to prevent any threats to users.[50]

Following the data protection law obligations that will be explored in detail in section 4, the protection of user informational autonomy will be considered at the planning stage of information-technological procedures and systems.[51]

From a different perspective, an overview of the horizontal EU consumer law *acquis* shows that many consumer regulations can address misleading and unfair design. Like data protection law, consumer law is

[47] Willett Chris, Martin Morgan-Taylor, 'Recognising the Limits of Transparency in EU Consumer Law' in James Devenney, Mel Kenny (eds), *European Consumer Protection: Theory and Practice* (Cambridge University Press 2012).

[48] Trzaskowski (n 49 Ch. I), 8.

[49] Mireille Hildebrandt, Beert Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73(3) Modern Law Review 428-460.

[50] On the Learned intermediary hand see, among others: Robert Cooter, Thomas Ulen (eds.), *Law & Economics* (5th edn., Pearson Addison-Wesley 2007).

[51] Bert-Jaap Koops, Ronald Leenes, 'Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision' (2014) 28 (2) Data-Protection Law International Review of Law, Computers & Technology 159-171, 161. For the Authors PbD 'implies that regulators should focus on achieving a privacy mindset rather than focus on hardcoding privacy'. Peter Schaar, 'Privacy by Design' (2010) 3 Identity in the Information Society 267-274.

aimed at strengthening consumer rights, with specific attention to their ability to make informed decisions. This is because even if the *New deal for consumers,* adopted by the European Commission in 2020, contributed to modernising the context and improving the enforcement tools for the new market features,[52] regulation is still rooted in the pivotal role of the informational approach.

The Directive on Unfair Commercial Practices (UCPD) and the Directive on Unfair Terms (UCTD) aim to reach fairness in the marketplace place and empowerment of collective entities and consumers accordingly. At the same time, the General Data Protection Regulation (GDPR) focuses on the rights and remedies of individual data subjects and enforcement through data protection agencies. It combines data protection with the free flow of data in the Internal Market.

As it will be further discussed in Chapter III, it is worth noting that in spring 2022, the Commission launched a Fitness Check of EU consumer law on digital fairness,[53] wishing to determine whether the existing fundamentala horizontal law (consumer and competitions laws) remains adequate for ensuring a high level of consumer protection in the digital environment.[54]

If we consider the fundamental value protected by the user's right to be informed, namely freedom of self-determination,[55] doctrinal and policy

[52] Commission Communication Delivering a New Deal for Energy Consumers, COM/2015/0339 final. Moreover, see the complete consumer protection framework at <https://ec.europa.eu/info/law/law-topic/consumer-protection-law/review-eu-consumer-law_it> accessed 10 June 2022.

[53] About the initiative of the Fitness Check on EU consumer law see <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413 Digital-fairness-fitness-check-on-EU-consumer-law_en>.

[54] ibid. The fitness check (evaluation) will look at the following pieces of EU consumer protection legislation to determine whether they ensure a high level of protection in the digital environment: the Unfair Commercial Practices Directive 2005/29/EC; the Consumer Rights Directive 2011/83/EU; the Unfair Contract Terms Directive 93/13/EEC. The Commission is gathering views and information on the key problems in this area, including possible solutions, and the scope for simplification and burden reduction. The planned timing of the Fitness Check enables the Commission to complete a comprehensive and evidence-based evaluation that takes into account the entry into application of the latest changes to these directives on 28 May 2022, resulting from the Directive on the Better Enforcement and Modernisation of Consumer Law (Modernisation Directive) and Digital Services Act, Digital Markets Act, Artificial Intelligence Act and Data Act.

[55] Recently in the field: Pixavra Vogiatzoglou, Peggy Valcke, 'Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU

questions flourish. All the questions are well summarised by the recent report of the European Consumer Organisation (BEUC) dedicated to the EU Consumer protection 2.0. Structural asymmetries in digital consumer markets,[56] which addresses (a) how consumers can be meaningfully informed about technically complex issues such as data collection online; (b) how realistic an informed consent approach in times of information overload and constantly divided attention; and (c) what role can GDPR and consumer law play in helping consumers to manage their data once consent has been given (post-consent management).[57] Given the timely considerations expressed within the document and the consequent ongoing debate, the Check will be scrutinised in Chapter III.

Indeed, the potential deviation that dark patterns can provoke between consumer choice and authentic preference is a circumstance that can hardly be demonstrated by the fundamental principle of the protection of freely given consent, both for the data-subject and the consumer entering a transaction.

In other words, the intense focus on informed consent as a legal basis for data processing in consumer transactions may not always provide optimal protection of digital consumer interests. Indeed, legal reasoning must also take into account the Unfair Commercial Practices Directive,[58] the Consumer Rights Directive,[59] and the Unfair Contract Terms Directive.[60]

law', in Ronald Leenes, Eleni Kosta, Irene Kamara (eds), *Research Handbook on EU Data Protection Law* (Elgar 2022) 11-50.

[56] BEUC (The European Consumer Organisation), 'EU Consumer Protection 2.0: Structural Asymmetries in Digital Consumer Markets', A joint report from research conducted under the EUCP2.0 project (2021) <https://dare.uva.nl/personal/pure/en/publications/eu-consumer-protection-20(81f5aca7-6b01-4ade-90fa-e02d3024bc3a).html> accessed 20 October 2022.

[57] ibid

[58] Parliament, Council Directive 2005/29/EC of 11 May 2005 (n 41 Ch. I).

[59] 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 (Consumer Rights Directive).

[60] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [2003] OJ L 95/29. Caterina Gardiner noted that UCTD pre-dates the advent of e-commerce, and although its provisions are principals-based and technology-neutral, the transparency controls have not been tested, nor are they well understood in the context of online presentation of standard terms. For a further analysis see Caterina Gardiner, *Unfair Contract Terms in the Digital Age* (EE Elgar 2022) 2.

The following subsections will explain how these different policies offers relevant principles and tools to this research. Before doing it, a few general remarks on the complex interplay between data protection law and consumer law will facilitate an understanding of the evolution toward their complementary and synergic roles (section 3.1).

3.1 A step back: the complex relationship between data protection law and consumer protection law

Notably, with the growth of the digital market, consumer protection and data protection have begun to overlap, becoming more and more complementary to one another. 'Payment by data' is, for example, just one of the most debated issues of the relationship between policies, as data processing becomes part of trader-consumer transactions.[61]

To understand the evolving path toward the matching points of the two policies, it is worth starting from their endemic differences and similarities.[62]

The constitutional foundations of each policy are different: data protection law is a fundamental right in itself, based on articles 7 and 8 of the Charter of Fundamental Rights of the European Union;[63] while the protection of consumer interests is the object of Art. 169 of the TFUE, and consumer protection regulation is still an internal market competence (ex Art. 114 TFUE).

Although data protection law in the processing of personal data grants rights to data subjects and imposes obligations on data controllers, the

[61] See Art. 3 of the Parliament Directive 2019/771 of 20 May 2020 on certain aspects concerning contracts for the supply of digital content and digital services (DCD) [2019] OJ L 136/1. Art. 3 states, for the first time, that the rules shall also apply to the 'consumer provides or undertakes to provide personal data to the trader'.

[62] Extensive recognition of the main differences and commonalities are presented by Dan Jerker B. Svantesson, 'Enter the quagmire – the complicated relationship between data protection law and consumer protection law' (2018) 38(1) Computer Law & Security Review 25-36; and Natali Helberger, Frederik Zuiderveen Borgesius, Agustin Reyna, 'The perfect match? A closer look at the relationship between Eu consumer law and data protection law' (2017) 54(4) Common Market Law Review 1427.

[63] For a critical analysis on the question if the right to personal data protection should be interpreted and enforced solely, or primarily, in relation to the right to privacy stated at Art. 8 CRF, see Plixavra Vogiatzoglou, Peggy Valcke 'Chapter 1: Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law' in Eleni Kosta, Ronald Leenes, Irene Kamara (eds.), *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022) 11.

rationale of consumer law is less clear because it does not immediately appear to protect a specific fundamental right. It should not be forgotten that the primary function of consumer law is market regulation, which implies the improvement of services and products offered by removing enterprises that remain in the markets just thanks to unfair commercial practices. Consumers' rights protection is instrumental.[64]

Generally observing, the object of a 'high level of consumer protection' stated in Art. 38 of the EU Charter of Fundamental Rights essentially responds to two different rationales: (i) to protect consumer rights and information, and (ii) to protect consumers in situations where they act as a weaker party. Data protection law and consumer law share common goals (e.g. to spread innovation and promotion of economic growth) and many legal tools to pursue these goals. An exemplary standard tool is informed consent: a functional means to addressing the so-called power asymmetry.[65]

Before the change of landscape previously described (section 3), consent was the legal basis for the lawful processing of personal data. At the sometime, consumer law added some more requirements to inform consumers when the personalisation of services, products and information was at stake.

The CRD, for example, focusing on digital content, requires companies to inform consumer about the tracking of consumer behaviour (recital 19, Art. 5 and 6 of the CRD). Theoretical analysis about the relationship between consent on data and its potential functionality to conclude a contract represents a key issue about the interconnection of data protection law and consumer law.[66]

Moreover, when GDPR came into force, the debate changed its perspective, as the regulation introduced an autonomous European discipline for the consent on data, entirely autonomous from the National

[64] Besides other Micklitz writings, see Hans-Wolfgang Micklitz, 'The Expulsion of the concept of protection from the Consumer Law and the Return of Social Elements in the Civil Law: a bittersweet polemic' (Working Paper) EUI LAW 2012/03.

[65] In data protection law, the formal requirements for consent are intended to be enforced by specialised government agencies. Michiel Rhoen, 'Beyond consent: improving data protection through consumer protection law' (2016) 5(1) Internet Policy Review 1-15.

[66] Among others see: Claudia Irti, *Consenso "negoziato" e circolazione dei dati personali* (Giappichelli 2021); Alberto De Franceschi, *La circolazione dei dati personali tra privacy e contratto* (Esi, 2017) 72; Giuseppe Versaci, *La contrattualizzazione dei dati personali dei consumatori* (Quaderni di «Studi Senesi», vol. 5, ESI 2020).

disciplines on consent, in all the other specific fields of private law.[67] The overarching (and overlapping) principles at the basis of GDPR constituted a sort of 'due diligence' process for data controllers[68].

Currently, concerns deal with the effectiveness of informed consent in all circumstances where digital manipulation needs to be faced.[69] For this reason, the following analysis of data protection regulation will first focus on the breach of consent situations as an essential tool to protect autonomy, before shifting toward the important role of design rules, as user-friendly information could help consumers (section 4).[70] The same concerns also shaped the structure of the analysis of consumer law (section 5).

As far as the scope of the two policies is concerned, the fact that consumer law aims at providing consumers with a sufficient level of protection (as a minimum standard) constitutes a remarkable difference; indeed, data protection law strikes an appropriate balance between the protection of personal data and the free movement of data.[71] While consumer protection law can be seen to set a 'floor' merely (minimum level) in its pursuit of a sufficiently high level of consumer protection, data protection law sets both a floor and a ceiling due to its articulated dual purposes of (a) protecting individuals regarding the processing of personal data and (b) providing for the free movement of such data.[72]

[67] Elise Poillot, 'La protection des données personnelles par le droit européen de la consommation', in Mathieu Combet (ed), *Le droit européen de la consommation au XXIe siècle. État des lieux et perspectives* (Bruylant 2022) 309.

[68] According to Jan Trzaskowski, the principles can be grouped in three pair: lawful processing (legitimacy, including proportionality); data controller's obligations (accountability, including security); data subject's rights (empowerment, including transparency). Jan Trzaskowski, 'GDPR Compliant Processing of Big Data in Small Business', in Carsten Lund Pedersen, Adam Lindgreen, Thomas Ritter, Torsten Ringberg (eds), *Big Data in Small Business – Data-Driven Growth in Small and Medium-Sized Enterprises* (Edward Elgar 2021). See also Trzaskowski (n 49 Ch. I).

[69] It is quite long time since scholars agree that information and mandate disclosure are not the solution for every problem. From the side of consumer law specialists, see: Geraint Howells, 'The potential and limits of consumer empowerment by information' (2005) 32 Journal of Law and Society 349.

[70] Rayn Calo, 'Against notice skepticism in privacy (and elsewhere)' (2013) 87 Notre Dame Law Review 1027.

[71] Svantesson (n 62 Ch. II), 30. The Author summarized this distinction affirming that: «consumers protection law merely sets the floor, data protection law sets both the floor and a ceiling».

[72] ibid

Consequently, data protection aims to address power differentials based, inter alia, on information asymmetries and bargaining power.[73]

For the current analysis, it is interesting to focus on the relationship between the two policies that provide consumers with more remedies in some circumstances.

It has to be considered that, ultimately, many consumer transactions for free online services enable companies to collect consumer data. It is possible that a breach of information requirement could also be interpreted as an unfair commercial practice, as depending on National law, the failure to provide information or misleading information could render the contract void. In such circumstances, it is consumer law that provides contractual remedies for the breach of transparency requirements.[74]

In many regulations, consumer policy states the priority of the *lex specialis* (e.g. Art. 3 of the Directive of Consumer Rights). On the other hand, the Preamble 42 of the GDPR describes itself as a *lex specialis* to guide how the rules provided by the Council Directive 93/13/ECC relate to unfairness apply to data. Moreover, regarding the provision of Article 1 of the GDPR, it has to be noted that consumer law can be limited by data protection law for reasons concerning the free movement of personal data.

Thus, under data protection law, limitations to consumer protection law are legitimized. Looking at the nature of this relationship, and with keen attention to the level of harmonization of European private law the legislator wishes to reach, Svantesson distinguishes two situations:

'1. If data protection law consciously aims to allow something, it is not appropriate for consumer protection law to forbid it but

2. If data protection law refrains from regulating a particular issue for the reason that it is already appropriately addressed by consumer protection law, then the data protection law's silence obviously does not constitute any obstacle for upholding the relevant aspect of consumer protection law'.[75]

Concretizing this theoretical vision within practical situations, the consumer and data protection frameworks of the European Union seem not to be functional to constraining anti-privacy design techniques

[73] David W. Slawson, 'Standard form contracts and democratic control of Lawmaking Power' (1979) 84 Harvard Law Review 529.

[74] This issue was observed by Helberger (n 62 Ch. II) 9. The GDPR often proves to be inflexible.

[75] Svantesson (n 62 Ch. II) 32.

embedded in websites that induce the consumers to entering into a contractual agreement which would not have happened without the use or influence of the dark patterns. However, the interaction between data protection law and consumer law will play a role against dark patterns. The UCPD Guidelines underlined it:

'a violation of the GDPR or of the ePrivacy Directive will not, in itself, always mean that the practice is also in breach of the UCPD. However, such privacy and data protection violations should be considered when assessing the overall unfairness of commercial practices under the UCPD, particularly in the situation where the trader processes consumer data in violation of privacy and data protection requirements, i.e. for direct market […]'.[76]

Thus, a data protection liability claim for dark patterns could potentially be pursued against a non-controller third party under consumer law. Potential pitfalls relating to traditional principles (e.g. transparency) will be discussed because they are central to the subject-matter in hand.

Insights about the need for a tighter (and clearer) synergy between the two policies and their enforcement tools.

4. The perspective of data protection law

Within the European data strategy drawn in Chapter I, the current analysis focuses on two specific evolving aspects of European data protection law which are crucially essential for protecting autonomy: (i) the advancement of the jurisprudential path, to understand if the GDPR overlooks how user 'clicks' can be manipulated by dark patterns, within the so-called Web 2.0 click-wrap ecosystem (section 4.1; 4.2); and (ii) the increasing role of the 'by design' provisions concerning to privacy, transparency, and fairness as they are crucial principles to prevent *ab origine* dark patterns (section 4.3).

Practically speaking, the first issue questions whether most empowerment mechanisms (e.g. notice and consent form) and principles currently employed are still effective. It investigates to what extent the effectiveness of informed consent, primarily guaranteed by the ePrivacy

[76] Commission, Staff Working document, Guidance on the interpretation and application of the Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market, 2021/C 526/01.

Directive specifically on cookies and direct marketing, and by articles 4, 5, 6, 7, 9 of the GDPR,[77], will still assure the fundamental requirements of a lawful consent through the analysis of the most recent EU case law in the data-driven digital context, and particularly in cases where consent on data was 'scraped' by machines, or obtained under dark patterns.

The GDPR gives little guidance on how information must be disclosed to individuals to meet the 'lawfulness, fairness and transparency' obligations under Art. 5(1)(a).[78] It is not the only provision which was identified as written in open-ended language.[79] The same wide definition is also adopted in Artt. 13-15, indicating that data controllers must provide data subjects with 'meaningful information about the logic involved'. In a context governed by algorithms, this last provision remains unclear and does not seem to contribute to implementing and guaranteeing the so-called 'algorithm transparency'.

Users are asked to consent in ways that comply with the requirements of the GDPR, assuming that this prerequisite will be sufficient to ensure protection of freedom of choice.

As the Guidelines 5/2020 on consent under Regulation 2016/679 underlined:

'generally, consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful'.[80]

[77] For a comprehensive explanation frame of the GDPR provisions dedicated to information and consent, see, among others, Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide* (Springer 2017).

[78] The Art. 5 (1)(a) states that the personal data shall be: «processed lawfully, fairly and in a transparent manner about the data subject ('lawfulness, fairness and transparency')».

[79] Katarina Foss-Solbrekk, Ann Kristin Glenster, 'The intersection of data protection rights and trade secrete privileges in "algorithmic transparency", in Eleni Kosta, Ronald Leenes (eds.), *Research Handbook on EU Data Protection Law* (Edward Elgar Publisher 2022) 163.

[80] EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679' adopted on 4 May 2020, 5, <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-

This is, however, often considered an optimistic view that does not correspond to what happens: the assumption of autonomous consumer, which is rooted on consumer protection law, cannot be inferred if the 'flow of information' is not transparent, complete, and free, or if it is so merely formally.

The GDPR provisions were written when dark digital architectures were not yet widespread, thus, still few studies addressed the importance of the contribution offered by behavioural studies to test the efficiency of consent.[81] Edwards noted that before the GDPR came into force, consent 'was a magic wand that could be waved by any popular online service to secure itself a revenue stream of personal data whilst remaining legally compliant'.[82]

Even after the Regulation went into force, the effectiveness of consent protection could have been significantly improved.

Nonetheless, the interpretative function of the European Court of Justice concretely determined to what extent the meeting of current GDPR requirements for freely given consent was still sufficient and suitable to cope with dark pattern challenges, especially when consent on data is an essential condition to conclude a contract (section 3.1).

4.1 A global view

Indeed, the intent to avoid the adverse effects of dark patterns on user consent is not exclusively a European goal. In various geopolitical contexts, lawmakers and regulators are starting to address the more pervasive contours of the data-driven economy, seeking operational solutions by, first and foremost, strengthening the protection of the information-related right of self-determination through the imposition of a duty of transparency upon those subjects responsible for data collection, storage, and processing.

The various approaches adopted in different jurisdictions to cope with dark patterns, for example updating existing legislation outlawing deceptive

052020-consent-under-regulation-2016679_en> accessed 10 June 2022. See also Article 29 Working Party Opinion 15/2011 on the definition of consent (WP 187), 6-8, and Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP 217), 9, 10, 13 and 14.

[81] Lucilla Gatt, Roberto Montanari, Ilaria Amelia Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 2 Politica del diritto 363-380.

[82] Lillian Edwards, *Law, Policy and the internet* (Hart Publishing 2019).

and fraudulent commercial practices in general; developing and promoting guidance on how current consumer law applies to dark commercial patterns; implementing bans on specific online commercial practices: developing voluntary standards or conducting business and consumer awareness campaigns.

In the US system, a lively doctrinal debate has long been ongoing on the adequacy of ordinary contractual remedies for users injured by unauthorized or unwanted data dissemination. The debate led to the presentation in the Senate of several Bills to address dark pattern usage, such as the Deceptive Experiences to Online Users Reduction Act (the so-called *Detour Act*),[83] which would lean on the Federal Trade Commission (FTC) powers to curb dark pattern usage.[84] The Act was recently incorporated into the 'American Framework to Ensure Data Access, Transparency, and Accountability Act' (The Safe Data Act),[85] which prohibits manipulating a user interface to compel compulsive usage.

Moreover, on September 15, 2022, the FTC released the report 'Bringing Dark Patterns to Light',[86] showing the increased use of sophisticated dark pattern designs by retailers intended to manipulate consumers into making decisions that benefit the retailers at the

[83] The US Deceptive Experiences to Online Users Reduction Act (the so-called Detour Act) introduced April 9, 2019, by Sens. Warner, D-Va., and Fischer, R-Neb.

[84] The U.S. Federal Trade Commission (FTC) is giving serious attention to the use of dark patterns by businesses. It issued a complaint against Age of Learning for its use of dark patterns involved with their service ABC Mouse. The FTC alleged ABC Mouse made cancellation of recurring subscription fees difficult for tens of thousands of customers despite promising 'easy cancellation'.

[85] Sen. Wicker, Roger F. [R-MS] (Introduced 07/28/2021). The Act is available at: https://www.congress.gov/bill/117th-congress/senate-bill/2499.

[86] FTC (staff report), Bringing Dark Patterns to Light, Sept. 2022, available at <https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf>. The report highlighted four common tactics: Disguising Ads which are designed to look like independent, editorial content; comparison shopping sites claiming neutrality that ranked companies based on compensation they received; countdown timers claiming that consumers had only a limited time to make a certain purchase that were not actually time-limited deals; difficult cancellation processes which are subscription sellers made extremely difficult to cancel despite touting 'easy cancellation' processes. For example, some subscription companies made the cancellation process very lengthy, requiring consumers to click through several pages of promotions, or hard to find. The report also found that some companies hid terms on key limitations on products or services in dense terms that consumers did not see before the purchase, and others advertised only part of a product's total price to lure consumers in and failed to disclose other mandatory charges until much later in the buying process.

consumer's expense. The report examined the use of dark patterns across various industries and contexts, including e-commerce, cookie consent banners, children's applications, and subscription sales. Companies offering consumer products and services should take heed of the FTC's report and ensure that their marketplaces do not employ the tactics identified by the report. Appendix A of the report describes more than 30 common dark patterns: a clear signal of the focus of future FTC scrutiny.

From a legislative point of view, on October 12, 2020, the State of California announced a new round of modifications to the *California Consumer Privacy Act* (CCPA),[87] including a new provision (Section 999.315(h) limiting the number of steps it takes for a consumer to opt out of the sale of personal information: they must be no more than the number of steps necessary for the consumer to opt into the sale. Additionally, the regulation also prevents a business from obliging the consumer to read a list of reasons not to opt out while trying to opt out (999.315(h)(3).

The requirements of transparency and informed consent are central to the current California Consumer Privacy Act (CCPA), which guards against the kinds of activities that dark pattern usage encompasses. Over time, this Act has been subjected to numerous amendments extending the protection because legislators have identified it as the appropriate tool to respond to new critical issues emerging from technological developments. Lastly, the *California Consumer Privacy Rights Act* (CPRA),[88] which took effect on 1 January 2023, has specifically defined dark pattern as 'a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice'. It also called out dark patterns in the context of valid user consent to data processing,[89] by

[87] State of California Legislative Counsel, Assembly Bill No. 375, Chapter 55, 2018.

[88] California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, available at <https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf>.

[89] Modifications to the CCPA were proposed in October 2020, among them: limiting the number of steps required for a consumer to opt out of the sale of their personal information (cannot require more than opt in does); prohibiting businesses from using confusing language to prevent consumer opt out; prohibiting businesses from requesting personal information from consumers trying to opt out when it is not necessary to complete the request; prohibiting businesses from forcing the consumer to read or listen to a list of reasons not to opt out while they are trying to opt out; prohibiting businesses from requiring consumers to search or scroll through a privacy policy, web page, etc. to

amending the existing *California Consumer Privacy Act* (CCPA) to include a specific mandate that 'agreement obtained through use of dark patterns does not constitute consent' under the CCPA (Section 1798.140(h), while Sec. 1798.185(a) indicates that the California General Advocate must ensure that the link used by providers to allow the opt-out option to the user does not employ dark pattern strategy.

The linguistic expression used in CPRA, as well as in other jurisdictions, as in Colorado with the Colorado Privacy Act[90], to define dark patterns echoes the proposed 2018 Detour Act. It defines dark patterns as a form of decisional interference, which presupposes that companies can improve the interference by presenting choices to their customers in a neutral way, or at least not inherently self-preferencing.

Indeed, in the U.S., for years, cases of data web scraping have been reported on the asserted violation of the Computer Fraud and Abuse Act (CFAA)*,*[91] initially enacted by Congress in 1986 to combat various forms of computer crimes, such as hacking and unauthorized intrusion into computer systems or databases.

Jurisprudential interpretation has also, historically, included under the protection afforded by the Act many forms of unauthorized access to sites and data. A notable case is Facebook v. Power.com,[92] where Facebook sued a small start-up – Power.com – that aggregated social media to access social media accounts through a unique interface. To do so, users had to provide their logins to Power.com, which accessed the accounts and extracting the data. In this case, the users were voluntarily granted their login information. On Facebook's appeal, the court found a violation of the CFAA by ordering the investment of the service offered by Power.com, thus, indirectly giving rise to the increase of Facebook's power which, in fact, assumed a dominant position.

Much like what happens in the US, with the California Privacy Rights Act (CPRA) signed into law on June 28, 2018, in Europe the discussion about dark pattern effects on consent have been conducted earlier under GDPR. In April 2019, for instance, the French data protection Authority, the Commission

find how to submit an opt out request when they have clicked 'Do Not Sell My Personal Information'.

[90] In the Colorado Privacy Act (CPA, SB21-190, 2021), dark patterns are defined as user interfaces designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

[91] Codified by 18 U.S. Code § 1030 (Fraud and related activity in connection with computers).

[92] *Facebook v. Power.com* C 08-5780 JF (Oct. 22, 2009).

nationale de l'informatique et des libertés (CNIL), released a report discussing the importance of user interface design on user empowerment.[93] The CNIL stressed the crucial role of design to protect privacy, and also discussed how consent that was gathered using dark patterns would not qualify as valid and freely given, stating 'the fact that using and abusing a strategy to divert attention or dark patterns can lead to invalidating consent'.[94]

4.2 Recent EU decisions on the effective protection of authentic will: Planet49, Orange Romania, and Meta/Facebook platforms cases

Over the years, case law and jurisprudential interpretation of GDPR have been decisive in measuring the effectiveness of the critical rules of informed consent and transparency. Therefore, this analysis considers recent European cases, mainly concerning the efficacy of online consent, outlining the actual trajectories of self-determination and informed choice protection in the data-driven context.

The whole aim of case law analysis conducted throughout this Chapter, even concerning consumer law and competition law cases, serves the function of understanding how judges assess the lawfulness of data exploitation strategies.

Starting from the rulings based on the key role of information and data process in securing freedom of choice, it must be recognized that European jurisprudence conveys well-established positions regarding for example the nature of consent on the disposal of data, as well as recent interpretative lines addressing the most innovative profiles on the subject, including the protection of data-subject victims of dark patterns, through scraping mechanisms of consent.[95]

Focusing on the prominent European cases about dark patterns which ruled on the basis of GDPR provisions, a well-known ruling regards implied consent, which occurs when one continues to use a website without actively objecting to a notice (or cookie): judges of Luxemburg

[93] Available at <https://www.cnil.fr/fr/definition/commission-nationale-de-linformatique-et-des-libertes-cnil> accessed 17 November 2023.

[94] CNIL, 'Shaping choices in the Digital World From dark patterns to data protection: the influence of ux/ui design on user empowerment', available at <https://www.cnil.fr/sites/cnil/files/2023-06/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf> accessed 13 June 2022.

[95] Particularly, for damages caused by dark patterns, specialized scholars built up useful websites that also collected case law from different jurisdictions. See the website: <https://www.deceptive.design/types> accessed 7 June 2023.

held that this circumstance do not establish a valid legal basis for data processing and collection, because it does not involve user action.

In the case of Planet49,[96] the ECJ Grand Chamber ruled on the active and unequivocal nature of consent. In the case at hand, a German company had used a preselected checkbox by which regular users who aspired to participate in sweepstakes expressed consent to installing cookies to collect information for advertising purposes.

To play in the lottery, users were required to tick a checkbox to receive third-party advertising otherwise they could not play. Also, the registration process included a pre-ticked checkbox that would allow tracking of their online behaviour. The court held that consent to the installation and consultation of cookies on the subject terminal equipment was not validly manifested through a preselected checkbox, which the user must, moreover, uncheck in order to deny consent to the processing of his or her data (para. 65). Furthermore, the ECJ stated that the possibility of unchecking the box is not an active action, but a passive one. In this case, the identified deceptive patterns were: preselection that employs the default effect of cognitive bias, based on which people tend to go with the option that is already chosen for them, even if there are other choices available; forced action, which involves a provider offering users something they want to compel them to do something in return; and sneaking (so users do not notice it happening because of obscuring information) or trick wording (to make the action seem more desirable than it is).

Due to the violations of Artt. 4(11) and 12 of the GDPR, the ruling is on the same wavelength as recital (32) GDPR, stipulating that 'silence, pre-ticked boxes or inactivity should not constitute consent'. The ECJ has helped identify the specific conditions under which consent is effectively free and informed to constitute a suitable legal basis for data processing; above all, it has to be expressed in a positive action, distinct from the activity the user wishes to pursue.

Thus, rulings with specific regard to cookie consent have also already been held by courts. When it comes to cookie consent management, dark patterns can also prevent effective consent in the sense of Article 5 (3) of the e-Privacy Directive.

Statements on this profile can be found at a national level as well. In France, for example, with the Délibération of 29 December 2022, TikTok

[96] Case C-673/17, *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* EU:C:2019:246 [2017].

was fined by the French Data Protection Authority for implementing advertising identifiers without consent and for having an insufficiently informative cookie banner.[97] The banner allowed users to accept all cookies with one click, making it difficult to refuse them. Some advertising cookies were placed even if a user did not consent. The case analysis involves TikTok's violation of Article 82 of the French Data Protection Act regarding its use of cookies and its cookie banner. The investigation by the French DPA found that TikTok's cookie banner did not provide users with enough information and options to give informed consent. The DPA identified several deceptive patterns that TikTok used, such as hard-to-cancel ('Roach Motel'), forced action, and hidden information, in its cookie banner.

Furthermore, in Germany, the opinions of the data protection supervisory authorities described practices like cookie consent under dark patterns as inadmissible nudging.[98]

Another area in which courts intervened is the withdrawal of consent. This operation should be as simple as providing it.[99] For a valid model, after consent is given, the same consent withdrawal form should be available at each access point, which is not always the case. In fact, in off-line reality such 'boxes', can be compared to the informed consent form used in medicine (formulary), which was evaluated as an invalid form of consent, even before the mid-1990s.[100]

[97] Commission nationale de l'informatique et des libertés, Délibération de la formation restreinte n°SAN-2022-027 du 29 décembre 2022 concernant les sociétés Tik tok Information Technologies Uk Limited Et Tiktok Technology Limited. The case is available at: <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046977994?page=1&pageSize=10&query=2016%252F679&searchField=ALL&searchType=ALL&sortValue=DATE_DECISION_DESC&tab_selection=cnil&typePagination=DEFAULT>. TikTok has been fined a total of €5,000,000 by the Data Protection Authority (DPA) for violating the General Data Protection Regulation (GDPR). The fine was divided into two parts – € 2,500,000 for failing to obtain valid consent from users and € 2,500,000 for displaying imprecise information on its consent banner.

[98] See DSK, OH Telemedien, 1 December 2021; LfD Niedersachsen, Handreichung: Datenschutzkonforme Einwilligungen auf Webseiten - Anforderungen an Consent-Layer, as of September 2022.

[99] About the revocation see Giorgio Resta, 'Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali' (2000) Riv crit dir priv 299.

[100] For example, Cass. Civ. 2 July -11 Nov. 2019, n. 28985, commented by Paola Frati, Armida Campolongo, Raffaele La Russa, *et al.*, 'Violazione del consenso informato: codifichiamo nozioni, significati e risarcibilità dei danni alla luce della pronuncia n. 28985/2019 della Suprema Corte di Cassazione' (2020) 4 Responsabilità civile e

Furthermore, the need for affirmative action that proves the user understands the disclosure has already been emphasised about the terminology used: consent mechanisms employing different visual techniques or colours for terms such as 'agree' or 'allow', and for terms such as 'reject' or 'block' are not legally compliant, as the system is influencing users to opt for the acceptance.[101]

Indeed comprehensible character must be intrinsic to the information, without which consent (even contractual consent) would be deprived of its authentic nature. A manifestation of will has to be free, conscious, and feeding, discouraging instead of increasing the so-called 'consent (and reading)-fatigue'.[102]

In Orange Romania,[103] the ECJ goes further than what it already did in the case of Planet49*,* analysing the active, freely-given, and informed nature of consent.

previdenza 1364-1384. Thus, recently clarified by the order of the Cass. Civ. – 10 June 2006 n. 11112.

[101] Available at UK Information Commissioner's Office: <https://ico.org.uk/>.

[102] The phenomenon of 'consent fatigue', where consumers are playing whack-a-mole with consent notifications without taking time to understand them. See BEUC (n 56) accessed 10 August 2023.

[103] Case C-61/19 *Orange România SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal* (ANSPDCP) EU:C:2020:901. On 11 November 2020, the Court of Justice of the European Union (CJEU) issued this decision in the case Orange Romania SA v. The Romanian National Supervisory Authority for the Processing of Personal Data (Romanian DPA). Orange România SA is a provider of mobile telecommunications services on the Romanian market. On 28 March 2018, the Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (national Romanian data protection authority; 'the ANSPDCP'), based on Article 32 of Law No 677/2001 (Romanian Data Protection Act) imposed an administrative penalty on Orange România (a provider of mobile telecommunication services on the Romanian market) on the ground that copies of the identity documents of its customers had been obtained and stored without their express consent. The DPA also ordered the controller to destroy already existing copies of the IDs. Orange România had requested consent for this data processing from its customers by giving them the opportunity to refuse their consent in handwritten form. Some of the contracts for mobile telecommunication services had a pre-ticked box signalling the consent to the storage of ID copies, while other did not. To sign that they do not give their consent to the storage of the ID copies, the customers had to fill out an additional form before the conclusion of the contract. In sum, the Court decided that a contract for the provision of telecommunications services which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document for identification purposes is not such as to demonstrate that that person has validly given his or her consent, as provided for in those provisions, to that collection and storage, where: (i) the box referring to that clause

Orange România SA, a provider of mobile telecommunications services in Romania, was found responsible for using pre-ticked boxes to obtain consent from customers for storing copies of their identity documents, which does not constitute active consent. The DPA found using of pre-ticked boxes to signal consent to the storage of ID copies was a deceptive pattern that violated the principle of 'freely given' consent.

About the active nature of consent, the ECJ states that the consent is not invalid if the pre-ticked box attached has been checked by the data controller before signing that contract.

As regards the freely given and informed nature of consent, the Court stated consent is not valid when the terms of the contract are capable of misleading the data subject, with the possibility of concluding the contract in question even if he or she refuses to consent to the processing of his or her data (para. 52). Consequently, forcing customers to complete another form to specify their refusal may confuse data-subjects, affecting their right to information.

Considering the decision from the business perspective, it could be challenging for them to raise the standards of consent, updating their consent collection practices to meet the ECJ requirements regarding consent.

Although Article 29 Working Party (WP29) has already shown that consent on data should not be a mandatory condition for the conclusion of a contract, the Court of Luxemburg goes further: it shows how the inclusion of additional conditions, for example, the completion of an additional form, leads to the invalidity of consent. In conclusion, in Orange Romania, the Court proposes a restricted vision, attributing an absolute value to consent when used as a legal basis for processing. Consequently, any restriction or formality, even negligible, could lead to the invalidity of consent. It significantly raises the standards of consent and will undoubtedly significantly influence in practice. It invites National courts to interpret consent to the highest standards.[104]

has been ticked by the data controller before the contract was signed, or where (ii) the terms of that contract are capable of misleading the data subject as to the possibility of concluding the contract in question even if he or she refuses to consent to the processing of his or her data, or where (iii) the freedom to choose to object to that collection and storage is unduly affected by that controller in requiring that the data subject, in order to refuse consent, must complete an additional form setting out that refusal.

[104] See for example the Cass. Civ. Order 14381/2021. The Italian Court of Cassation has gone so far as to assess the content of the information in cases of automated decisions (ex Article 22 GDPR), in relation to the application of Articles 13(2)(f) and 14(2)(g) of the

Notably, a relevant European interpretative proceeding on fundamental issues about consent was expected for a long on the well-known German Facebook (now Meta Platforms) case,[105] where the Bundeskartellamt has imposed far-reaching restrictions on Facebook in the processing of user data.[106] This ECJ decision come on 4 July 2023 (C-252-21),[107] where the Court of Justice resolved the problem around the potential interaction between data protection regulation and competition law following the legal opera that started in 2019 with the German competition authorities on the Meta case.

Before this ruling, according to Facebook terms and conditions, users were only been able to use the social network under the precondition that Facebook could also collect user data outside of the Facebook website on smartphone apps and assign this data to the user's Facebook account. All data collected on the Facebook website by Facebook-owned services such as WhatsApp, Instagram and other third-party websites, have been combined and assigned to the Facebook user account. For the German authority, Facebook-owned services, like WhatsApp and Instagram, can continue to collect data. However, assigning the data to Facebook user accounts will only be possible with the express voluntary consent of the user. Where consent is not given, the data must remain within the respective services, and cannot be processed in combination with Facebook data. Moreover, if consent was not given for data from Facebook-owned services and third-party websites, Facebook will have to restrict its collection and combining of data substantially.

With the appeal of the decision by Facebook,[108] the Düsseldorf Higher Regional Court refers questions to the ECJ as, for the German Court the

GDPR. The Court has, in these circumstances, clarified that in the event of an automated process, it is important that the user is informed about the logic used by the algorithm if it significantly affects his or her person.

[105] Facebook changes its name in Meta Platforms on October 28, 2021.

[106] Bundeskartellamt, 6 February 2019, B6–22/16 – Facebook.

[107] Case C-252-21 *Meta Platform and Others* (General terms of use of a social network). [2023] EU:C:2023:537.

[108] Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd., Facebook Deutschland GmbH v. Bundeskartellamt, intervener: Verbraucherzentrale Bundesverband e.V. For a comment, see: Francesco Laviola, 'Il diritto all'autodeterminazione informativa tra concorrenza e data protection. Riflessioni a margine della saga Facebook c. Bundekartellamt nella giurisprudenza delle corti tedesche e in attesa della Corte di Giustizia', in Elia Cremona, Francesco Laviola, Valentina Pagnanelli (eds), *Il valore economico dei dati personali* (Giappichelli, 2022) 27. See also

question of whether Facebook is abusing its dominant position,[109] as a provider on the German market for social networks (because it collects and uses the data of its users in violation of the GDPR) cannot be decided without the ECJ interpretative decision because the Court is responsible for the interpretation of European law.[110]

Leaving the competition legal aspects to section 6, the analysis focuses here on Facebook's ability to gather data on users via third-party sites (where it deploys plug-ins and tracking pixels) and across its suite of products (Facebook, Instagram, WhatsApp, Oculus), to its market power – asserting this data – gathering is not legal under EU privacy law as users are not offered a choice. This was expected to conduct the ECJ to definitively clarify the validity of consent when it constitutes an essential condition for concluding a contract.[111]

While the decision of the ECJ was pending, on 20 September 2022, the relevant Opinion of Advocate General Rantos was delivered,[112] indicated his position, attributing a remarkable value to a detailed case-by-case analysis of the various clauses of the Meta/Facebook terms of service, since it was impossible to establish whether, in respect of that practice, 'an

Karin Jackwerth, 'Great expectations: the Facebook case and subsequent legislative approaches to reregulate large online platforms and digital markets' (2022) 13 JIPITEC 200 para 1.

[109] See section 6.

[110] Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany.

[111] Precisely, with the third question of the request, the Dusseldorf Court wants to know whether a company, such as Facebook, can rely on Art. 6 (1) b) and f) GDPR when it combines Facebook Data and Off Facebook Data for personalising content and ads, data security, improving its services and a seamless use of products within Facebook group services (i.e. the Purposes). With its fourth question of the request, the Dusseldorf Courts asks whether a company such as Facebook can rely on Art. 6 (1) f) GDPR when it connects data from its own services or third party websites and apps, such Facebook Data and off Facebook Data to (1) process personal data of minors for the purposes (relevant when minors sign up to Facebook without the approval of legal guardians, which is deemed to be necessary for a valid contract according to German legal scholars); (2) provide statistics and analysis to other companies for their benefit (e.g. analysing campaigns that companies are running on Facebook); (3) communicate with users for direct marketing purposes; (4) use data for research purposes (e.g. understanding important social topics like perceptions about climate change); (5) inform public authorities about criminal offences, illegal use of services, violations of guidelines, etc.

[112] Opinion of advocate general Rantos, delivered on 20 September 2022, Case C-252/21 Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd., Facebook Deutschland GmbH v. Bundeskartellamt, intervener: Verbraucherzentrale Bundesverband e.V.

undertaking, such as [Meta Platforms]' can comprehensively rely on all (or some) of the grounds set out in Article 6(1) of the GDPR, even though it is possible that said practice, or some of its component activities, may, some instances, fall within the scope of that article'.[113]

Furthermore, in Rantos' words the processing envisaged by the cited provisions is carried out based on the general conditions of the contract imposed by the controller, in the absence of data-subject consent, or even against his or her will, would call for a strict interpretation, particularly in order to avoid circumvention of the consent requirement.

Keen attention is, likewise, dedicated to the role of the controller since under Article 5(2) of the GDPR, he is responsible for demonstrating that the personal data is processed in accordance with the regulation. Moreover, under Article 13(1)(c) of that regulation, the controller must specify the purposes of the processing for which the personal data is intended, as well as the legal basis to act.

As far as the interpretation of Article 6(1)(b) of the GDPR (the third question of the Dusseldorf Court directed to the ECJ) is concerned, the Advocate general considers the question of the lawfulness of data processing to the extent that it is necessary for the 'performance' of a contract to which the data subject is a party (there must be realistic, less intrusive alternatives, considering the reasonable expectations of the data subject. Where the contract consists of several separate services or elements of a service that can be performed independently of one another, the applicability of Article 6(1)(b) of the GDPR should be assessed in the context of each of those services separately).

As far as the personalised content is concerned,[114] and according to the case-law of the Court of Justice, the Opinion underlines that the provision in question (Art. 6 GDPR) lays down three cumulative conditions based on which the processing of personal data is lawful: first, the pursuit of a legitimate interest belonging to the data controller, or to the third party or parties to whom the data is disclosed; second, the need to process personal data for the purposes of legitimate interests pursued; and third, the

[113] ibid

[114] For that examination, consideration should also be given to the fact that the practice at issue concerns the processing not of data relating to the user's activities on the Facebook site or app, but data originating from external and therefore potentially unlimited sources. The advocate general questions to what extent the processing might correspond to the expectations of an average user and, more generally, what 'degree of personalisation' the user can expect from the service he or she signs up for. See Opinion, (n 112).

fundamental rights and freedoms of the data-subject do not take precedence.

Ultimately, the Advocate general noted that it is unclear whether, and to what extent, Meta Platforms Ireland has explained – for each purpose of processing, and type of data processed – the actual legitimate interests pursued, or other justification that may be relevant. Consequently, the ECJ examines to what extent, in the circumstances described, the practice is justified by the existence of legitimate interests of Meta Platforms Ireland in the processing of data within the meaning of Article 6(1)(f) of the GDPR or by any other condition laid down in Article 6(1)(c), (d) and (e) of that regulation.

The proposed solution consists of interpreting Article 6(1)(b), (c), (d), (e) and (f) of the GDPR as meaning that the practice at issue, or some of the activities that comprise it, may be covered by the exemptions laid down in those provisions, as long as each data processing method examined fulfils the conditions provided for, by the justification specifically put forward by the controller, therefore: (i) the processing is objectively necessary for the services relating to the Facebook account; (ii) the processing is necessary for the legitimate interests pursued by the data controller, or by the third party to whom the data is disclosed and does not have a disproportionate effect on the fundamental rights and freedoms of the data subject; (iii) the processing is necessary to respond to a legitimate request for specific data, to combat harmful behaviour and promote security, to conduct research and to promote safety, integrity and security.

With the decision of July 4, 2023, the Court of Justice follows word by word, AG Rantos' Opinion. The Court of Justice remarks that although compliance with the GDPR does not pre-empt the finding of an abuse, it can be considered within the 'all-of-the-circumstances' analysis and, in this context, it may even be a vital clue to assess whether the conduct entails resorting to methods prevailing under merit-based competition (AG Rantos Opinion, para 23). However, the Court of Justice adds that this element may also be assessed to draw out the consequences of a certain practice in the market or for consumers (para 47). By doing so, however, the Court of Justice remarks that NCAs are not replacing the role of data protection supervisory authorities because they do not act within the powers and tasks conferred upon them under Articles 51(1) and 57 of the GDPR (para 49).[115]

[115] With these words Alba Ribera Martínez commented the new ruling on July 5, 2023, available at: <https://competitionlawblog.kluwercompetitionlaw.com/2023/07/05/getting-

Lastly, looking at the consistent number of judgments, the ECJ grants the consumer the right to provide ex post factum consent to standard terms that do not comply with EU law. Consent may legitimize the abstract unfairness of the standard term. The presumption is that consent proves that the consumer knows and understands what they are consenting to.

'It will have to be shown that consent can only justify abstract unfairness if a whole series of safeguard measures are established so as to guarantee consumer autonomy'.[116]

This is particularly evident when consumers are minors. The EDPB decision 2/2022, for example, fined Meta Platforms Ireland Ltd for failing to provide processing contact information on children's business accounts and using 'public by default'-settings for child users by preselection and sneaking patterns.[117]

clued-into-the-interplay-between-data-protection-regulation-and-competition-law-in-case-c-252-21-meta-platforms-and-others-conditions-generales-dutilisation-dun-reseau-social/> accessed 8 July 2023.

[116] BEUC, 'EU Consumer Protection 2.0 - Protecting fairness and consumer choice in a digital economy' (2022) available at <https://www.beuc.eu/position-papers/eu-consumer-protection-20-protecting-fairness-and-consumer-choice-digital-economy> accessed 12 May 2022.

[117] European Data Protection Board (Edpb), Binding decision 2/2022 on the dispute arising on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instragram) under Article 65(1)(a) Gdpr, adopted on 22 July 2022. The Irish Data Protection Commission (DPC) found that Instagram's default account settings for child users were set to public, meaning that anyone on the app or website, regardless of whether they were registered users or not, could view the contents of the account. This was in violation of Article 12(1) of GDPR, because Instagram did not clearly and transparently inform child users of the purpose of public-by-default processing. Although Meta (Instagram's parent company) had informed child users of this setting in their 2018 and 2020 Data Policies, the DPC deemed this insufficient. The EDPB agreed with the DPC's assessment that the interests pursued by Instagram were not specific enough, as the controller had mentioned them in vague language. The EDPB also criticized the DPC for not conducting a better evaluation of the existence of the legitimate interest(s) pursued by Instagram. Furthermore, Instagram failed to provide child users with information on the purposes of processing and the categories of recipients of personal data using clear and plain language, which was required under Articles 13(1)(c) and (e) of GDPR. Following the adoption of a binding decision by the EDPB, the Irish DPC fined Meta € 405,000,000 for processing contact information on children's business accounts without legal grounds and for having default settings set to 'public' for child users. More details are available at: <https://www.deceptive.design/> accessed 15 May 2003.

4.3 Web-scraping personal data in online platforms: insights from recent American litigation

Although many cases remain problematic, both at the regulatory and jurisprudential interpretative levels, there is a recent US trend aimed at circumscribing situations of web scraping to be sanctioned.

The landmark case was ruled on April 18, 2022; the U.S. Court of Appeals for the Ninth Circuit ended a long legal battle led by LinkedIn to prevent the rival company,[118] HiQ Labs, from using its user public profiles data (web scraping) to detect and analyse professional relationships.[119]

Unlike the Power.com case (see section 4), the Ninth Circuit Court reaffirmed its original decision, denying that the extraction of data about

[118] In general, US cases concerning dark patterns are numerous. Among others, it is useful to mention a case that identified the following dark patterns: hidden subscription; hard to cancel; sneaking. It is the case decided by the US District Court of California, Federal Trade Commission v. Age of Learning inc. (ABCmouse.com), Case No. 2:20-cv-7996, available at <https://www.ftc.gov/system/files/documents/cases/1723186abcmouseorder.pdf> accessed 13 July 2023. Age of Learning operates a membership-based online learning tool called ABCmouse Early Learning Academy for children between two and eight years old. ABCmouse failed to clearly disclose to consumers that their subscriptions would renew automatically, leading to additional charges and made it difficult for them to cancel their memberships. The company also failed to disclose important information related to negative option plans, including the total amount consumers would be charged if they did not act to cancel the deadlines by which they must cancel to avoid unwanted charges.

[119] To sum up, LinkedIn served HiQ with a cease-and-desist, demanding that HiQ cease its activity of accessing and copying data from LinkedIn's server. HiQ filed suit against LinkedIn, seeking both injunctive relief under California law and a declaratory judgment to prevent LinkedIn from lawfully invoking the Computer Fraud and Abuse Act (CFAA), the Digital Millennium Copyright Act (DMCA), California Penal Code § 502(c), or the common law of trespass against HiQ. The Ninth Circuit held that there was no abuse of discretion by the district court where the court had found that even if some LinkedIn users retained their privacy despite their public status, as they were not scraped, such privacy interests did not outweigh HiQ's interest in maintaining its business. In balancing the hardships, the Ninth Circuit weighed in favor of HiQ. Further, the Ninth Circuit noted that HiQ posed serious concerns with regards to 'the merits of its claim for tortious interference with contract, alleging that LinkedIn intentionally interfered with its contracts with third parties, and the merits of LinkedIn's legitimate business purpose defense'. *United States Ninth Circuit, hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019). LinkedIn petitioned the Supreme Court to review the Ninth Circuit's decision and in a second ruling, in April 2022, the Ninth Circuit affirmed its decision (hiQ Labs v. LinkedIn Corp., 31 F.4th 1180 (9th Cir. 2022). Then, the lower court in August 2022 issuing an order dissolving the preliminary injunction, and the most recent mixed ruling on November 4th, 2022.

LinkedIn users, available with public access by the company Hiq Labs violated the Computer Fraud and Abuse Act, CFAA.

The 9th Circuit found that HiQ's business model depended by LinkedIn publicly accessible data and rejected LinkedIn's argument that it considered HiQ could gather workforce data from other means. It also rejected LinkedIn arguments that allowing HiQ to scrape LinkedIn's site threatened its user privacy and put at risk LinkedIn's goodwill with its members.

In other terms, regarding LinkedIn's economic interests – avoiding competition from third parties that also want to profit from selling its users' data – the Court held that LinkedIn:

'has no protected property interest in the data contributed by its users, as the users retain ownership over their profiles'. Users, moreover, entirely evidently intend their profile data to be accessed by others «including for commercial purposes'.

The significant difference from its predecessor Power.com, lies in the public nature of user data: HiQ, for example, does not need to access LinkedIn through a log-in process to dispose of user data.

It should be considered that the Court of Appeal judgment came after the Supreme Court decision HiQ Labs, Inc. v. LinkedIn Corp, which asked for reconsideration of the case in light of the famous Van Buren decision. This case occurred the previous year, when the Court had preempted itself on interpretive dissimilarities with the federal law, the Computer Fraud and Abuse Act, 18 U.S.C. Section 1030 (CFAA) aimed, inter alia, to protect workplace computers, and the information stored in them, from various types of unauthorized accesses, whether by employees, as occurred in the Nathan Van Buren plaintiff case (an affair known as Van Buren's 'gates-up-or-down inquiry'), or by former employees or competitors.

In sum, this U.S. Supreme Court case dealt with the Computer Fraud and Abuse Act (CFAA) and its definition of 'authorized access'. In June 2021, the Supreme Court ruled on the 'exceeds authorized access' to files and other information in connection with intentional access to a computer system that one is otherwise authorized to access. The CFAA language had long created a rift in case law, and the Court decision narrowed the applicability of the CFAA in prosecuting cybersecurity and computer crimes.

Therefore, following the Van Buren precedent,[120] in LinkedIn v. HiQ, the Ninth Circuit Court of Appeals rejected LinkedIn interpretation, noting that the CFAA is best understood as an 'anti-intrusion' law and not as an Act based on the concept of 'misappropriation', so where the case involves a site with public access, the CFAA is not violated.

The Court notes that the CFAA contemplates the existence of three types of computing 'scenarios': (1) computers for which access is open to the general public and authorization is not required; (2) computers for which authorization is required and has been granted, and (3) computers for which authorization is required but has not been granted (or, in the case of the prohibition against exceeding authorized access, has not been granted for the part of the system being accessed).

Public profiles on LinkedIn are available to anyone with an Internet connection, and they fall into the first category. As for websites made freely accessible on the Internet, the analogy to 'trespassing' often invoked during congressional consideration does not apply, and the requirement of authorization is inadequate.

This case has significant privacy implications. It sets a precedent about the fact that data entered by users to a social media website does not belong to (but rather is merely licensed to) the site owner. It undermines the significance of user agreements to set the terms for non-users who might collect and use data made available on those sites, in contradiction of the agreement terms. It also narrows the definition of 'authorization', in the context of websites that collect and host personal data, to those sites that require usernames and passwords and increase the responsibility of such websites to inform users of privacy settings benefits.

The case returned to the district court for a trial on the merits, while in the meantime, in November 2022, a settlement agreement was reached between the two parties.

4.4 Regulation by design: the contribution of the GDPR

Data protection law has the merit of integrating individual rights into the data systems' operations because the concept of 'data protection by design' is enshrined in the GDPR: it constitutes the most direct way to discipline the design, avoiding the use of circumvention techniques that endanger the effectiveness of techno-regulatory measures.

[120] *Van Buren v. United States* 940 F. 3d 1192 No. 19-783 (2021).

The idea to shape legal policies starting with the design phase of the technology, mainly through the functions of algorithms, concerns several specific profiles such as transparency by design, safety by design and competition by design,[121] all broadly derived from the concept of 'data protection by design' (PbD). This last concept is explicitly recognized in Art. 25(1) of GDPR[122], according to which system designers need to consider the privacy risks of their digital architectures as early as possible and throughout the entire process.[123]

Based on PbD, controllers implement data protection principles, accountability and fairness into the data processing design. Practically speaking, through this mechanism, data protection becomes part of data processing, even when the complex techniques for personal data processing are not fully comprehended by users. Concerning to the more traditional data protection approach based on ex post remedies, the design approach shifts to a proactive and preventive perspective.[124]

[121] Margrethe Vestager, 'Algorithms and competition', Speech at the Bundeskartellamt 18th Conference on Competition (Berlin, 16 March 2017).

[122] Art. 25 GDPR states: «taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. The controller shall implement appropriate technical and organisational measures to ensure that, by default, only personal data necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the storage period and accessibility. Such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. An approved certification mechanism pursuant to Article 42 may be used to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article».

[123] Ann Cavoukian, 'Privacy by Design - The 7 Foundational Principles, Information and Privacy Commissioner of Ontario' (2009) <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf> accessed 20 July 2022.

[124] The idea of embedding privacy safeguards in information systems and other technology types goes to the 90s. The EU Data Protection Directive already contains several provisions that expressly call for implementing of technology safeguards in the design and operation of information systems. Article 17 lists the data controllers' obligation to implement appropriate technical and organisational measures to protect

The European Data Protection Board (EDPB) adopted the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (version 2.0), underlining the necessity for data controllers to implement GDPR obligations when designing processing operations. Moreover, EDPB gives guidance on appropriate measures to provide effective implementation of Art. 25 obligations. Thus, the controller must understand data protection principles and the data-subject's rights and freedoms to properly implement the legal requirements as early as possible. The key elements dealing with the characteristics of the content are inspired to clarity, semantics, accessibility, relevance, comprehensibility, and the universal design multi-channel. This last one is relevant to facilitating the enforcement of rights, as well as the avoidance of discrimination.[125] Often, in fact, companies, such as Tinder or Facebook, recognise the GDPR user rights, but they do not enough to enforce design architectures pragmatically at the light of GDPR rights.

Commentary on the guidelines underlined deceptive practices which are contrary to both the data protection by design, and by default obligations.[126] By adopting a design pattern that unduly impedes the free choice of data subjects, data controllers would fail to fulfil their duty to implement appropriate technical and organisational measures effectively manner. In some instances, this might even constitute a violation of the transparency principle, andthe lawfulness principle, and consent given via manipulative patterns cannot be considered 'freely given' and thus cannot serve as a valid legal basis for the data processing in question.

Clear and plain communication with data subjects regarding the processed data is an essential condition with other interconnected European principles: fairness and lawfulness. This is why a related issue of data protection is transparency, which is also, despite many weaknesses, a

personal data. The Directive, however, has not been sufficient in ensuring that privacy is adequately embedded in information systems.

[125] Edpb, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, adopted on October 20, 2020': <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf> accessed 15 September 2022.

[126] Jiahong Chen, Derek McAuley, Ansgar Koene, 'Comments on the European Data Protection Board's Guidelines 4/2019 on Article 25 Data Protection by Design and by Default' (2020) <https://nottingham-repository.worktribe.com/output/3774977> accessed 8 January 2023.

core concept of the GDPR,[127] and its enforcement by design can better contribute to avoiding dark patterns.[128]

More precisely, transparency is, on the one hand, connected to the accountability of controllers for mandatory information (Articles 12, 13 and 14 of the GDPR) and, on the other hand, to the accessibility of information, the provision of meaningful choices, and the reduction of information vulnerabilities. The twofold structure of the principle of transparency (temporal and formal requirements), similar to the way it is described in the consumer field, can be retrieved in data protection law as well: the General Data Protection Regulation (GDPR) requires that the mandated disclosures listed at Article 13 GDPR (i.e. the essential information about the processing that has to be given to the data subject when personal data are directly obtained from her) has to be provided at the moment of the collection of personal data.[129]

As far as formal requirements are concerned, the GDPR echoes the consumer protection rules: the data controllers shall take appropriate measures to provide the information required by law (Articles 13-14 GDPR) and any communication regarding the right of access, the use of automated individual decision-making, and personal data breach, as well as to present the request of consent: 1) in a concise, transparent, intelligible and easily accessible form; 2) using clear and plain language; 3) provided in writing or by other means, including, where appropriate, by electronic means; 4) provided orally, if requested so by the data subject.

[127] There are transparency obligations to controllers in multiple Articles: Articles 5, 12, 13, 14, 26, 40, 41, 42, 43, 53 and 88 and in Recitals 13, 39, 58, 60, 71, 78, 100 and 121 GDPR. Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679 (2017).

[128] This possible solution is also presented by Luiza Jarovsky, 'Transparency by Design: Reducing Informational Vulnerabilities Through UX Design' (May 25, 2022) <DOI:10.2139/ssrn.4119284>. The Author discusses the mismatch between what the law requires, what data controllers are offering, and what data subjects need, is that data subjects are left vulnerable. Data subjects do not have suitable information accessible to them or meaningful choices, and they do not know about their data protection rights. They are left unaware of what is happening to their personal data and what they can do to change it.

[129] Where the information is derived from third party sources (which is the case enshrined at Article 14 GDPR), the information duties have to be fulfilled: 1) within a reasonable period, depending on the specific circumstances of the processing, which cannot exceed in any case one month; 2) if the personal data are intended for communicating with the data subject, at latest at the occurrence of the first communication; if the data controller plans to disclose the personal data, at latest at the time of the first disclosure (Article 14.3 GDPR).

The main goal of 'transparency by design' is that data subjects will be served with meaningful and actionable information, instead of a standard block of text that acts as a liability document for the controller mission. Data subjects are vulnerable and manipulable and need protective measures not to be exploited by controllers. For this reason, transparency by design establishes that (a) controllers have to transmit a set of information to data subjects and to facilitate the exercise of data protection rights ('accountability') and (b) this must be done in a timely, adequate and accessible way and through the promotion of meaningful privacy choices, in order to reduce the informational vulnerabilities that enable dark patterns and unfair privacy policies ('fairness').

To promote fairness, one of the aspects related to transparency obligations in the GDPR, the controller must be aware of the key design elements that compose a privacy choice, choosing mechanisms that can mitigate the data subject's information vulnerabilities.

Indeed, hypothesizing the implementation of transparency by design, it means focusing on accountability and fairness (see more in Ch. III).[130] Design would be indispensable to complying with transparency obligations, as it should embed values and premises and empower data subjects throughout their interaction with the controller.

Transparency by design would embrace privacy by design by sharing the same principles. It must be noted that transparency moves forward from the privacy issue in the sense that it is not only a matter of data protection but also an issue of consumer law regarding its view of the individual and his or her decision-making model. To meet the obligation of fairness in terms of conditions, online platforms must design, organize, and operate their interfaces to avoid deceit, manipulation and other material distortion or impairment of their user's ability to make free and informed decisions (see more section 4.1).

For the GDPR, visualization and iconography (Art. 12.8 GDPR) are indeed means to guarantee transparency, similar to the food labelling regulation. The literal and formal importance given to these aspects was not accompanied by adequate pragmatic indications differently from what happened in the transparency principle with WP29.

It should be noted that in recent times, private forms of regulation, such as private voluntary standards and soft law have contributed significantly to enriching the content of the principle of transparency.

[130] Gianclaudio Malgieri, 'The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation' (2020) 20 Proceedings of Fat 27.

WP29, which issued the final version of its guidelines on transparency under Regulation 2016/679 in April 2018, influenced the interpretation and applicability of the GDPR remarkably. Concretely, the working group WP29 delineates general principles, clauses, and practical indications as the succinct and efficient way to present information and to implement transparency as a 'user-centric [concept] rather than legalistic'.[131]

WP29 seeks to guarantee that the consumer has the suitable tools to foresee the scope, the potential risks, and the consequences of the data process, also in line with judicial decisions on consumer law. Overall, the guidelines also benefit the behavioural empirical insights expressed by the behavioural economy.[132]

The interdisciplinary key to understanding mandated disclosures and transparency become central: empirical findings from linguistics, information design, human-computer interaction, and behavioural sciences (no matter which specific science it originates from: psychology, neurosciences, sociology) can efficiently contribute to shaping the content of the principle of transparency, providing not only ex ante guidance to traders and data controllers, but also a toolkit to enforcement authorities and courts to assess ex post the respect of legal obligations.[133]

Based on these keen scholars' observations, the design approach, as a way of proactively thinking, reveals itself as an effective tool for coherently applying these new directions in complying with transparency. Consequently, patterns operatively translate the legal principle of transparency into practice through behavioural and design lenses (see Ch. III).[134]

[131] Point 4 of the document (Guidelines on transparency under Regulation 2016/679).

[132] Precisely, the Guidelines on transparency under Regulation 2016/679 emphasized the fact that controllers are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/notices/ policies etc., they can test these, for example, through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies, where appropriate, amongst other things (ibid, point 9 of the doc.).

[133] Arianna Rossi, Rossana Ducato, Helena Haapio, Stefania Passera, 'When Design Met Law: Design Patterns for Information Transparency' (2019) vol. 122-123 (5) Droit de la consommation 79-121, available at <http://hdl.handle.net/2078.1/216263> accessed 15 May 2022.

[134] ibid

5. The perspective of consumer law

This section explores to what extent consumer law is synergic with data protection law when it protects transparency and assesses fairness and lawfulness for consumption choices. To this end, the paragraph focuses on implementing and application of the key clauses of transparency, and the fairness test, with specific attention to the impact of UCPD (section 5.2) and of the new Digital Market Package (section 5.1). These requirements are formally essential for fair communication and substantial lawful contents.

Dark patterns are transforming consumers 'from service recipients to servants of the data industry companies'.[135] This critical change emerges in public and political discussions. During the Roundtable on digital dark commercial patterns held in 2021, the OECD analysed the growing range of 'dark commercial patterns' and highlighted the difficulties in distinguishing them from other marketing techniques.[136] Nevertheless, progress in legal literature was not yet ready to identify the dark patterns individually, the OECD already outlined a way to distinguish dark commercial patterns from other persuasive marketing techniques: the former could modify choice architecture to hamper consumer decision-making, through changes to the decision space or manipulation of information flows, as well as their potential for individual and collective consumer welfare loss.

The OECD final document was in line with a few National experiences, as for example, in Norway, where starting in 2018, the Consumer Council, a very active consumer group in the field of digital rights, published a report on how default settings and dark patterns are

[135] Speech by Giovanni Buttarelli, 'Dark patterns in data protection: law, nudging, design and the role of technology' at Legal Design Roundtable, 29 April 2019, Brussels, Belgium.

[136] OECD (2021), Roundtable on Dark Commercial Patterns Online: Summary of discussion, available <https://one.oecd.org/document/DSTI/CP/CPS(2020)23/FINAL/en/pdf>. The document reported that in a sweep conducted in 2019 by the International Consumer Protection Enforcement Network (ICPEN) of 1760 websites/applications of retail businesses across a range of sectors, 429 (24%) were flagged for potential 'dark behavioural nudges'. The top three dark nudge practices identified were: pressure selling (e.g. using scarcity claims), drip pricing, and design issues such as obscuring terms and conditions. Another study conducted in 2019 by academic researchers from Princeton University in the United States identified 1,818 instances of dark commercial patterns (falling into 15 categories) in a crawl of around 11,000 retail businesses and online marketplaces websites. Such patterns have also been identified on social media platforms and other websites to promote fraudulent advertising directing consumers to counterfeit and other illicit products.

used by tech companies such as Facebook, Google and Microsoft to nudge users towards privacy intrusive options.[137]

Describing many of the tactics that will be later classified as dark patterns, the OECD framed the related concerns into consumer law. It underlined that there are several options to respond to the large number of practices that are considered dark commercial patterns: for example, authorities might treat 'disguised ads', which are generally viewed as deceptive under consumer laws in most OECD jurisdictions, differently from 'confirmshaming', which might present more novel issues of law.

Indeed, these OECD observations imply the acknowledgement that dark patterns remarked ongoing challenges and changes in consumer law. Likewise, to the constraints shown by the information normative paradigm already discussed,[138] politicians are digging deeper into 'choice architecture and default settings surrounding personal decisions that might cause consumers to choose differently and better'.[139] Personalized commercial practices, such as personalized advertisements and pricing, already showed this mechanism.[140] In general, structural and digital asymmetry will be widely discussed in Chapter III.[141]

The most heated debate revolves around consumer digital contracts: the principle of transparency implies that pre-contractual information has to be provided in advance and presented in compliance with substantial and formal requirements. Timing information requires that the consumer must be able to gain knowledge of the terms before entering a contract. In

[137] Consumer Council 'Deceived by Design: How tech companies use dark patterns to discourage us from exercising our right to privacy' (2018) <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-designfinal.pdf>; Norwegian Consumer Council (2018), 'Every Step You Take: How deceptive design lets Google track users 24/7', available <https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-everystep-you-take.pdf>. It follows the: Norwegian Consumer Council, 'Out of Control: How consumers are exploited by the online advertising industry' (2020) available at <https://fil.forbrukerradet.no/wp-content/uploads/2020/01/202001-14-out-of-control-final-version.pdf> accessed 11 April 2023.

[138] See the implications driven by the sociology of consumption studies: Lois W. Hofman, *Developmental psychology today* (McGraw-Hill, 1994).

[139] Hans W. Micklitz, Lucia Reisch, Kormelia Hagen *et al.*, An Introduction to the Special Issue on 'Behavioural Economics, Consumer Policy, and Consumer Law' (2011) 34 J Consum Policy 271-276.

[140] Article 29 Data Protection Working Party Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (2017) <https://ec.europa.eu/newsroom/ article29/items/612053>.

[141] BEUC (n 102).

some specific contract law areas, the legislator establishes some information design requirements: for example, in distance contracts, the main elements of the contract have to be ‘displayed in the close vicinity of the confirmation requested for placing the order’ (recital 39, CRD), in order to ensure that the presentation of information allows the user to become acquainted with the terms effectively.

The UCTD rationale focus on transparency based on the traditional view that informed consumer will make decisions to maximize their welfare. ECJ has already confirmed that the lack of transparency is a factor that must be considered when assessing the fairness of terms under Art. 3 UCTP.[142] There is a gap in the UCTD as to the consequence of breach of the transparency requirement has resulted in considerable legal uncertainty (the rule only applied when the clause is contra proferentem). Indeed, it was observed that are transparency principle under UCTP can only be applied to ambiguous terms, but based also on Study for the Fitness Check of EU Consumer and Marketing Law it is still not clear what terms can be considered unfair about online contract resulted from preliminary commercial practices (e.g. exaggerated use of hyperlinks that could conduct to the so-called ‘wrap contracts’) which could play a role in the opposite direction of the one aiming at achieving market transparency.[143]

The modality to express information for example, is crucial as it can reveal a sort of indirect manipulation: transparency means to inform in a clear and intelligible manner, so that the ‘average consumer’ can understand without legal advice.[144]

Such a requirement is difficult to grasp as both UTD and CRD usually provide comprehensive statements, underling the need of a ‘plain and intelligible language’, where intelligibility also stands for the legibility of that information.

Soft law instruments offer more detailed guidelines about the presentation of information.

For example, the 2021 Guidance document about the CRD contains a model for the displaying consumer information about digital products.[145]

[142] Case C-472/10 *Nemzeti Fogyasztòvédelmi Hatòsàg v. Invitel. Tàvkozlesi Zrt* [2012] EU:C:2012:242.

[143] See Caterina Gardiner, *Unfair Contract Terms in the Digital Age. The Challenge of Protecting European Consumers in the online Marketplace* (EE Elgar, 2022) 100.

[144] The concept of ‘average consumer’ is widely analysed in Ch. III.

[145] Commission, ‘Guidance of 29 December 2021 on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights’ [2021] OJ C 525, 1-85. The Notice replaces the Guidance document on the Consumer

Interestingly, the Guidelines document encourages the use of icons, tables, structured layout, and other graphical elements to illustrate the content of a contract. However, the model is not binding, refers to online products only, and serves as a mere exemplification to suggest alternative and more user-friendly ways to present information to the trader without setting specific criteria.

Plain and intelligible language has been broadly interpreted by the European Court of Justice.[146] As a precondition, information must be formally and grammatically intelligible. Consumers must be able to evaluate the legal and economic consequences of choices by considering all the elements of the transaction, including the marketing process, and reasonable expectation of attention from the average consumer.[147]

In certain areas, Member States are called upon to enforce consumer rights. For example, one of the areas that could require further legal regulation is online video games. Dark pattern are mentioned in the European Parliament's resolution of 18 January 2023 on consumer protection in online video games.[148] The Resolution indicates the need to strengthen consumer protection against the availability of video games that can be sold using game designs, commonly known as dark patterns, which could have harmful psychological and financial consequences through unwanted or uncontrolled purchases, especially for minors and young children (there is an ongoing court case in the Netherlands on the measures to apply to loot boxes; Slovakia is also investigating the appropriate measures to take). This lack of a harmonised approach leads to the fragmentation of the market for video games within the EU, and there are no specific consumer protection mechanisms at European level to ensure the protection of all players, particularly minors and young children, as regards paid loot boxes.[149]

Rights Directive from 2014. It is available at <https://commission.europa.eu/law/law-topic/consumer-protection-law/consumer-contract-law/consumer-rights-directive_en> accessed 10 October 2022.

[146] About the plain and intelligible language see: Case C-472/10 *Nemzeti Fogyasztdvidelmi Hatdsdg v Invitel Tvkozlesi Zrt* [2012] ECLI:EU: C:2012:242, para. 27

[147] For more details on the topic see Rossi, Ducato, Haapio, Passera (n 133).

[148] Parliament, Report of 19 December 2022 on consumer protection in online video games: a European single market approach, A9-0300/2022.

[149] Parliament, 'Resolution of 18 January 2023 on consumer protection in online video games: a European single market approach' [2023] 2022/2014(INI), available at <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0008_EN.html> accessed 1 June 2023. The Resolution states at point 16: 'notes that, beyond in-game purchases systems and paid random items, other deceptive designs also occur in video games and can

5.1 Digital Services Act and the Digital Markets Act: Advantages and critics for the dark patterns ban

Based on empirical studies, companies use different tactics to prevent customers from quitting the subscribed service: these techniques often are forms of dark patterns.[150]

Dissuading customers from leaving the website is believed to increase the likelihood that they will re-engage. At the same time, companies can still benefit from customers, even if they are no longer active users, because companies have stronger legal grounds to keep using the data collected through user accounts. Therefore, maintaining access to existing user data is becoming more relevant as it becomes harder for firms to collect data about users due to nascent privacy initiatives.

This empirical data needs to be analysed from the perspective of the general governance of the digital market introduced by European Institutions with the legislation package composed of the Digital Services Act (DSA) and the Digital Markets Act (DMA). On 20 January 2022 the European Commission passed the final amendments, and the Acts constitute some of the most significant reform of internet platforms legislation in recent times. Mainly, DSA explicitly addresses design, indicating it can constitute an unlawful practice.

As a general overview, the DMA is aimed at ensuring fair competition between online businesses, limiting the market behaviour of so-called gatekeeper companies to ensure fair digital market. In contrast, DSA ensures the conditions for innovative digital services in the internal market. It also contributes to online safety and the protection of fundamental rights, setting a robust and durable governance structure for effectively supervising of intermediary service providers.

Although the DSA is not expressly structured to protecting consumers,[151] several provisions indirectly realised this objective (e.g. the

distort consumers' behaviour; calls on national authorities to effectively enforce European and national consumer protection laws, in particular the Unfair Commercial Practices Directive, and the corresponding guidance thereon, which prohibits certain dark patterns, aggressive marketing practices and misleading transparency on information that is required to be provided to consumers; calls furthermore on the Commission to continue assessing these issues, in particular dark patterns, as part of the ongoing fitness check on EU consumer law on digital fairness and to present adequate initiatives if deemed necessary'.

[150] Empirical findings are proposed by Runge, Wentzel, Huh, *et al* (n. 5 Introduction).

[151] Users can be consumers and firms. DSA aims to harmonise conditions for innovative cross-border services to develop in the EU, address and prevent the emergence

handling of harmful online content, the protection of online users' fundamental rights, and restrictions on the collection of personal data for advertising purposes and limitations on online behavioural advertising).[152] To meet the universal obligation to fairness, online platforms must design the organisation and operation of their interfaces in a way that avoids material distortion or impairment of their user's ability to make free and informed decisions.

DSA is qualified as a *lex specialis* that complements sector-specific instruments.[153] The complementary nature of GDPR is evident when it comes to the right of information, precisely when Arts. 12-1 integrates articles 12 to 14 GDPR, also regarding the additional transparency and accountability to targeted advertisement provided by articles 24 and 30 of the Act without prejudice to the rights and remedies available to data subjects. On a different side, the complementarity of DSA with EU consumer acquis is evident with the expressed references to Directive 93/13/EEC, Directive 98/6/EC, Directive 2005/29/EC and Directive 2011/83/EU, all amended by Directive (EU) 2019/21, and the maintenance of the approach already taken by the e-Commerce Directive.

While the specific rules on consumer-facing practices remain applicable (e.g. the Unfair Commercial Practices Directive), the DSA effectively legislates a general clause against misrepresentation and aggressive practices in all horizontal relationships that are not covered in any sector-specific legislation. The only requirement is that the practices must be conducted via apps, websites or other surfaces operated by online platforms that are not small or micro.[154]

of obstacles to these activities, and provide for adequate supervision to the provided services. It ensures that digital service providers are not misused for illegal activities and that operators act responsibly. See Morais Carvalho, Jorge, Arga, Lima, Francisco, Farinha, Martim, 'Introduction to the Digital Services Act, Content Moderation and Consumer Protection' (2021) 3(1) Revista de Direito e Tecnologia 71-104.

[152] Aina Turillazzi, Federico Casolari, Mariarosa Taddeo, Luciano Floridi, 'The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications' (2022) available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4007389> accessed 10 February 2023.

[153] Edpb, 'Opinion 1/2021 of the 10 February 2021 on the Proposal for a Digital Services Act', available at: <https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf> accessed 10 July 2023.

[154] The online platforms are also subject to an obligation to ensure a high level of privacy, safety, and security of minors on their services. Martin Husovec, Irene Roche Laguna, Principles of the Digital Services Act (Oxford University Press, Forthcoming 2023), available at <https://ssrn.com/abstract=41537966> accessed 30 June 2023.

Given its broader applicability to all online 'intermediaries' (from internet service providers and hosting services to messaging apps, email providers, and Amazon-style marketplaces), the DSA has drawn more attention to dark patterns. [155] According to recital 67, dark patterns aim to prevent users from making autonomous and informed choices or decisions. In contrast to UCPD, the trader's intention may – according to the wording of the recital – also play a role. However, the trader's intention is usually more challenging to determine than the architecture and the typical reaction of the average user. Recital 67 is less about the content of (e.g. advertising) statements, but primarily about the 'structure, design or functionalities' of online interfaces (i.e. primarily websites or apps), for example, because the choices are not presented neutrally, in that certain choices are given more prominences through 'visual, auditory or other components' – a topic, that was recently discussed above all by data protection supervisory authorities in connection with cookie banners. Also mentioned is the practice of repeatedly asking a user to resubmit a choice they have already made or making it more difficult to cancel than logging in, making default settings difficult to change, and misleading users by enticing them to make certain transactions. Besides, recital 51(b) expressly refers to the term 'dark patterns' on four occasions.

Thus, in line with its goal of protecting EU fundamental rights (freedom of expression and of information), a key area of reform under the DSA is in relation to dark practices, which are online service providers use to nudge, or pressure, users towards making decisions.[156] The DSA has banned providers of intermediary services from using deceiving or nudging techniques on recipients of their services; and from using dark patterns to distort or impair user autonomy.

DSA appears to break new legal ground with the explicit prohibitions of dark patterns in Articles 25, titled 'Online interface design and

[155] In its amendments to the (then proposed) DSA, the European Parliament Committee on the Internal Market and Consumer Protection (IMCO) added a recital (39a), in which we read: 'However, certain practices typically exploit cognitive biases and prompt recipients of the service to purchase goods and services that they do not want to reveal personal information they would prefer not to disclose.' Parliament, 'Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' [2021] A9-0356/2021 available at <https://www.europarl.europa.eu/doceo/document/A-9-2021-0356_EN.html> accessed 25 May 2023.

[156] Franz Hofmann, Benjamin Raue (eds.), *Digital Services Act. Gesets über digitale Dienste* (Nomos, 2023) 434.

organization' and 31 DSA, titled 'Compliance by design': they both set up decisive criteria to declare user freedom of choice is distorted or impaired by dark patterns. Indeed, Article 25 (para 1) prohibits online platform providers from designing, operating, or organising their online interfaces in a way that deceives or manipulates users or otherwise impairs their ability to make free and informed decisions.[157]

Upon first reading, this language may seem ambitious and far-reaching, but it is notable insofar as who it leaves out.

The apparently broad prohibition on efforts to interfere with user autonomy and choice is laid out in this Article. Based on it, the Commission may issue guidance on the application of paragraph 1 to specific practices, notably:

(a) giving more prominence to certain choices when asking the recipient of the service for a decision;

(b) repeatedly requesting a recipient of the service to make a choice where such a choice has already been made, especially by presenting a pop-up that interferes with user experience;

(c) making the procedure of terminating a service more difficult than subscribing to it.[158]

Researchers have a brood consensus: the three patterns are generally called 'asymmetric choice', 'nagging' and 'hard to unsubscribe'. While these three patterns are widely prevalent and can cause direct consumer harm, they do not include many common deceptive practices currently employed by online platforms. The DSA explicitly focuses on these three patterns, suggesting that the initial focus on dark pattern prohibition will centre on a relatively narrow range of manipulative practices.

By specifying that the prohibition on such deceptive design tactics applies only to online platforms, the drafters of the DSA opted to scope

[157] Art. 25 (1) states providers of online platforms shall not design, organise, or operate their online interfaces in a way that deceives, or manipulates, the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions. Art. 25 (2) introduces the exception for practices covered by Directive 2005/29/EC and Regulation (EU) 2016/679. Art. 25 (3) grants the possibility to the Commission to issue guidelines on how paragraph 1 applies to specific practices, notably: (a) giving more prominence to certain choices when asking the recipient of the service for a decision; repeatedly requesting that the recipient of the service make a choice where that choice has already been made, especially by presenting pop-ups that interfere with the user experience; making the procedure for terminating a service more difficult than subscribing to it.

[158] Art. 25 para (2) *sub a); b); c)*.

down the legal potential impact on the use of dark patterns. Consequently, does not effect on a wide range of intermediary services, including businesses foundational to online commerce, such as ISP's, web-hosting services, and domain name registrars. Other concerns of the ban regard what practices are affected.

Lastly, many of today's most prolific dark patterns do not announce themselves in the form of an annoying pop-up or even in a static user interface. Rather, they may manifest in dynamic, personalised interfaces that are driven by machine-learning algorithms honed through the ongoing collection of data. In terms of fighting manipulative algorithms, the DSA goes where U.S. regulators have yet to tread so far. Article 26, for example, requires huge online platforms to diligently identify, analyse, and assess systemic risks stemming from the design, including algorithmic systems, functioning, and use of their services and to conduct risk assessments.

DSA has already been criticized in several aspects. Some consider recital 67 overoptimistic considering the wording of Art 25.[159] Others emphasised that the aforementioned Art. 25 has a significant impact on dark patterns regulation, because it stipulates that the prohibition of dark patterns does not apply to the practices covered by the UCPD and the GDPR: DSA is a merely subsidiary prohibition alongside a broad definition of dark patterns.[160] Indeed, being a *lex specialis* that complements sector-specific instruments means, for example, to integrate GDPR, precisely when Art. 12-1 integrates articles 12 to 14 GDPR, also regarding the additional transparency and accountability to targeted advertisement provided by Artt. 24 and 30 of the Act without prejudice to the rights and remedies available to data subjects. DSA fails to establish clear criteria to distinguish illegal practices from legitimate ones (although that was a concern in recital 51b) and makes the concrete regulation of dark patterns dependent on EU guidelines.

Essentially, neither the GDPR, nor the Unfair Commercial Practices Directive have succeeded in broadly reining in dark pattern. As these two

[159] According to Jan Trzaskowski, recitals should to provide the reasons for the main provisions and should not contain normative provisions or political exhortations. Trzaskowski (n 51 Ch. I).

[160] ELI (drafters: Marie Jull Sørensen, Peter Rott and Karin Sein), Response (n 11), page 9 of the document. Incidentally, the document reminds on the fact that the Court of Justice has already recognized the potential application of different and multiple sanctions to the same conduct, e.g. Case C-453/10 *Pereničová and Perenič*, 15 March 2012, ECLI:EU:C:2012:144, para. 47. The point relate the use of unfair terms that can simultaneously constitute an unfair commercial practice.

laws do make room for regulating dark patterns, enforcement has been relatively weak and constrained to narrow contexts, such as cookie consents. Depending on how regulators interpret the DSA, this framing could have, or not have, profound implications on how gatekeeper future architectures are presented to consumers. A design that asymmetrically emphasizes one choice over another, for example, by highlighting a decisional button through size, colour, or both and leaving the other deemphasized or greyed out, will likely be deemed 'non-neutral', especially if it emphasizes a choice with economic or data disclosure impacts for the user.

With regards to the Digital Market Package, recital 63 puts a particular focus on one well-known dark pattern barring gatekeepers from making it 'unnecessarily difficult or complicated for business users or end users to unsubscribe from a core platform service'.[161] Article 13(6) DMA prohibits, as a matter of anti-circumvention, making the exercise of particular rights or choices 'unduly difficult, including by offering choices to the end user in a non-neutral manner, or by subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof.' Finally, the ban on dark patterns was also provided by Art. 70 of the DMA,[162] which is directed only to gatekeepers and only within the context of attempts to circumvent other obligations put in place by the law. However, many small companies that are also guilty of exploiting harmful dark patterns, often relying upon interface-based deception as a core aspect of their business models.

In conclusion, if the Digital Market Package represents a step forward with the expressed ban, the extension of the protection is still limited. It only applies to 'gatekeeper' companies, and only in contexts where those dark patterns relate directly to the other provisions. For example, a gatekeeper couldn't be able to use a dark pattern to solicit user consent to

[161] This recital is likely directed primarily at Amazon, given the Norwegian Consumer Council findings and complaint against Amazon regarding the challenges of unsubscribing from Amazon Prime.

[162] Gatekeepers should not engage in behaviour that would undermine the effectiveness of the prohibitions and obligations laid down in this Regulation. Such behaviour includes the design used by the gatekeeper, the presentation of end-user choices in a non-neutral manner, or using the structure, function, or manner of operation of a user interface, or a part thereof to subvert or impair user autonomy, decision-making, or choice.

receive targeted advertising. When significant actors like Amazon utilize dark patterns, the effects are felt at scale by many millions of customers.

5.2 The key role of unfair commercial practices directive

Data exploitation strategies could be regarded as potentially aggressive, or misleading practices and consequently unfair.

This can be exemplified by widespread problem mainly affecting the flight sector[163], where platforms often engage consumers in deceptive practices by hiding additional fees and violating laws related to commercial practices (the additional fees are only added once the consumer proceeds to the booking page and are not disclosed upfront).[164]

Debating this hypothesis, stakeholders consider the scenario where the prohibition of these strategies puts an end to commercial practices that aim to collect data and process it for purposes that the consumer cannot understand.

Unfair data practices exploit informational and cognitive vulnerabilities. Many of those practices match the unfair commercial practices regulated by the Directive 2005/29/EC (UCPD), as amended by the Directive EU 2019/2161. For this reason, it is essentially important to investigate if and to what extent the UCPD contributes to safeguarding individual transactional decisions in circumstances of technology-driven manipulation, maintaining a maximum harmonization where Member

[163] The duties imposed to the gatekeeper platforms by the Digital Markets Act (were relevant n 56, Chapter I). See also the Commission, 'Notice – Guidance on the interpretation and application of Article 6a of Directive 98/6/EC of the European Parliament and of the Council on consumer protection in the indication of the prices of products offered to consumers' C/2021/9328 OJ C 526, 29.12.2021, 130-140.

[164] The key player Airbnb that was held liable for the violation of Article 7(4)(c) of Directive 2005/29/EC UCPD, which requires traders to provide the total price when consumers are presented with an invitation to purchase. Airbnb was held liable for not disclosing additional fees upfront and violating commercial laws regarding hidden costs and upfront disclosure of the total price of accommodation. As a result of negotiations between EU Commission and Airbnb, the platform has improved and fully clarified how way it presents accommodation offers to consumers, which is now in line with the standards set in EU consumer law. Airbnb successfully addressed the demands of the European Commission and national consumer protection authorities, led by the Norwegian Consumer Authority, and implemented changes to comply with EU consumer rules. Airbnb and Consumer Protection Cooperation Network under the facilitation of the European Commission and the lead of the Norwegian Consumer Authority, Press release 11 July 2019.

States must not enact stricter rules.[165] The UCPD shares the principles of empowerment, proportionality and transparency with the GDPR. However, differently from the latter, it does not refer to the requirements for legitimacy, accountability and security.

Extending its ambit beyond mere information policy,[166] UCPD allows consideration of the reaction of an average 'targeted' consumer, which leads to difficulties when seeking to incorporate insights from behavioural economics: the practice is prohibited if it 'causes or is likely to cause' the average consumer 'to take a transactional decision that he would not have taken otherwise' (Art. 6, 7, and 8). A general prohibition of commercial practice is only by the UCPD if it is listed in Annex I of banned practices. All other practices are investigated on a case-by-case basis.[167]

Unfair commercial practices have an essential role in assessing the fairness of business-to-consumer commercial practices, and other instruments in the European framework, such as the eDirective, the GDPR or sector specific legislation applicable to online platforms. Indeed, the UCPD shares the principles of empowerment, proportionality and transparency with the GDPR, but the UCPD does not have similar requirements for legitimacy, accountability and security.

Based on Art 3(1) UCPD, the regulation applies to commercial practices during and after a commercial transaction,[168] and during a pre-contractual phase, where dark patterns usually manifest. It means it covers the advertising, sales and contract performance stages, including the agreement to the processing of personal data the use of personal data for

[165] Mateja Durovic, *European Law on Unfair Commercial Practices and Contract Law* (Hart Publishing, 2016).

[166] Catherine Barnard, Steve Peers (eds.), *European Union Law* (Oxford University Press, 2023) 730.

[167] Case C-13/15, *Criminal proceedings against Discount SA*, EU:C:2015:560, para 19.

[168] Case law provides a broad interpretation of the scope of 'transactional decision', as does the wording of Article 2(k) itself. In Trento Sviluppo and Centrale Adriatica v Autorità. Garante della Concorrenza e del Mercato, Centrale Adriatica launched a special promotion in several COOP Italia supermarkets. This case may have several implications. First, a broad interpretation of transactional decisions provides better protection in dark pattern scenarios; clicking and browsing the web or interacting with the interface should all be within the scope of a 'transactional decision' under the UCPD. Second, it is a typical case of promising or showing something intended merely as bait'; such practices may be comparable to dark patterns such as 'Bait and Switch' or 'Disguised Advertisement.' 'Bait and Switch' refers to practices that manipulatively navigate consumers away from their original intention regardless of their will.

delivering personalized content, and the termination of a contractual relationship.

As clarified by the Commission Notice with the Guidance on the interpretation and application of Directive 2005/29/EC,[169] published in 2021, the scope of the directive is broad: it can also cover commercial practices such as capturing consumer attention, which results in transactional decisions such as continuing to use the service (e.g. scrolling through a feed), to view advertising content or to click on a link.[170]

There are already several attempts to classify dark patterns with taxonomies that utilise the classification structure proposed by the UCPD.[171] The attempts show that the current unfair commercial practices list needs to be updated. The debate on dark patterns is not the first occasion this exigence was emphasised. The UCPD was in fact, the piece of legislation most affected by the changes introduced by the already mentioned Directive 2019/2161,[172] which broadened the object of the regulation, including not only goods and services but also digital services and digital content (e.g. practices dealing with advertorials and ranking of offers, ticket reselling and two practices related to the online reviews), and consequently adapting it to the particularities of the rising digital market[173]. Moreover, as aforementioned, DMA and DSA will

[169] Commission, 'Notice – Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market' [2022] OJ C 526, 1-129.

[170] ibid. With this note the Commission clarified its views on how the Directives apply to digital practices such as dark patterns and data-driven personalization.

[171] Mark Leiser, Wen-Ting Yang, 'Illuminating Manipulative Design: From 'dark Patterns' to Information Asymmetry and the Repression of Free Choice Under the Unfair Commercial Practices Directive' (2022) <https://doi.org/10.31235/osf.io/7dwuq> accessed 21 July 2022. The Authors summarise the corresponding UCPD provision or case-law for four categories under the 'Free Choice Repression' category: 'Pressure Imposing,' 'Forced Acceptance,' 'Undesirable Imposition' and 'Undesirable Restriction.' In general, dark patterns that fall within these categories have aggressive characteristics. Compared with the regulation on 'Information Asymmetry,' the law on the 'Free Choice Repression' dark patterns seems relatively fragmented. Some identified rules have a narrow scope and may only refer to certain specific practices rather than a general regulative capacity. Not all 'Pressure Imposing' dark patterns would be considered aggressive. Only severe dark patterns such as constant entanglement, serious insults, exploiting misfortune, or circumstances of such gravity as to impair the consumer's judgement, should be considered unfair.

[172] Parliament, Council Directive (EU) 2019/2161 (n 41 Ch. I).

[173] Durovic (n 3 Ch. III).

interact with the UCPD to access the average consumer test (see section 5.1).

Currently, there are some scholars' attempts to identify the architectural correspondence between some types of dark pattern and unfair commercial practices: there are, for example, dark patterns practices belonging to the information asymmetry category that could fall within the provisions of Articles 6, 7, and the Annex I (Blacklist).

The unfair nature implied in the asymmetry could be represented when clause: (i) provides incorrect information, (ii) withholds certain critical information, and (iii) provides or presents information misleadingly to deceive consumers. The practice of 'free choice repression' could be included in Articles 5, 8, 9, and Annex I; or the absence of information transparency would unfairly unbalance the relationship between consumers and traders.

There are various degrees of severity of manipulation.

Dark patterns, such as confirm shaming, could be included in Articles 8 and 9 UCPD if (1) the trader uses threatening or abusive language to manipulate consumers or (2) exploits a specific misfortune or circumstance to influence consumer judgements. Also, undue influence exists when a trader exploits a position of power about the consumer to apply pressure if it is 'likely to significantly impair the average consumer's freedom of choice or conduct' (Art. 9 UCPD).

New hypotheses of unfair commercial practice require testing the efficacy of the current fairness test, as the following paragraph will take into account (see section 5.3).

Pragmatically, within the marketing field, the personalisation of services or advertisements may lead to the exploitation of traditional and emerging users' vulnerabilities: EU consumer law contains significant barriers to effectively addressing such misuse.[174] Personalised marketing communication encompasses different communication techniques, all involving interactions between companies and consumers, data collection and processing by companies and delivering marketing products.[175] This is the reason why, to date the behavioural targeting of consumers falls into the nexus of data protection, competition, and consumer law. At this intersection of laws lie normative concerns about

[174] Joanne Strycharz, Bram Duivenvoorde, 'The exploitation of vulnerability through personalised marketing communication: are consumers protected?' (2021) 10(4) Internet Policy Review 1.

[175] ibid

balancing social welfare, the preservation of consumer choice, and the creation of trust within the internal market.[176] It offers consumers several benefits, such as increased relevance and credibility of communication, but at the same time, by targeting personal characteristics, such tactics make individuals more susceptible to persuasion. They blur the lines between persuasion and manipulation: this can be seen as a threat to individual autonomy and a risk for economic harm[177].

For example, online behavioural advertising, based on inferential analytics to target consumers based on data about their online behaviour, can amount to a misleading action or a misleading omission according to Articles 6 (misleading action) and 7 (misleading omission) UCPD, as well as an aggressive practice according to Article 8 (aggressive practice) UCPD.[178]

Consequently, in cases where these personalised tactics are related to a contractual or, more generally, a commercial intent, the UCPD applies and prohibits these practices based on the average consumer benchmark. It also provides that the unfairness of practices is likely to affect only a group of consumers who are particularly vulnerable to the practice, because of their mental or physical infirmity, age or credulity in a way that the trader could reasonably be expected to foresee, shall be assessed by the impact on the average member of that group.[179]

With the study conducted by the BEUC on the concept of digital vulnerability about the UCPD,[180] researchers have suggested that in digital markets the vulnerable consumer is no longer the exception, nor is the average consumer the rule. Instead, every consumer could be considered to have a persuasion profile, making them more or less vulnerable to certain practices and at specific times (See Chapter III). As it will be further demonstrated in the following chapter, case law, too, contributes to

[176] Johann Laux, Sandra Wachter, Brent Mittelstadt, 'Neutralizing Online Behavioural Advertising: Algorithmic Targeting with Market Power as an Unfair Commercial Practice' (2021) 58(3) Common Market Law Review.

[177] Federico Galli, 'Online Behavioural Advertising and Unfair Manipulation Between the GDPR and the UCPD' in Martin Ebers, M. Cantero Gamito (eds.), *Algorithmic Governance and Governance of Algorithms* (Springer International Publishing, 2021) 109-135.

[178] Laux, Wachter, Mittelstadt (n 14 Ch. II).

[179] Article 5 (3) UCPD.

[180] Helberger, Lynskey, Micklitz, Rott, Sax, Strycharz (n 159 Ch. I). EU consumer protection 2.0: Structural asymmetries in digital consumer markets [Position Paper]. BEUC. The European Consumer Organisation. <https://www.beuc.eu/publications/beuc-x-2018-080_ensuring_co nsumer_protection_in_the_platform_economy.pdf>.

a great extent to investigating the 'images of consumer' as a current benchmark because they form the foundations for various EU policies oriented towards the goal of consumer protection.[181]

The realistic picture of dark patterns' impact on the UCPD framework has to be completed by acknowledging the already quoted report recently published by the European Commission, entitled 'A behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalization':[182] the overall purpose of the study is the identification of problematic business-to-consumer commercial practices used in the digital environment, in particular manipulative personalization. Remarkably, the report, based on experimental studies, underlines that in terms of protective measures against unfair practices:

'the transparency-based remedies are ineffective for countering dark patterns and manipulative personalization practices for average and vulnerable consumers. Instead, remedies that have more potential for reducing consumer detriment include the prohibition of the most harmful practices, which are not yet blacklisted in Annex I of the UCPD or other EU legislation, and the imposition of a fair/neutral design obligation on traders. Furthermore, the distribution of the burden of proof or argumentation may have to be rethought to rebalance systemic digital asymmetries. However, remedies should go beyond regulatory interventions and involve businesses and the designer community directly, for example by developing guidelines and practical examples, which allow them to determine ex ante whether the practices that they are considering may be unfair' (see more in Ch. III).[183]

In sum, the recent study report for the Commission and empirical data testified that the traditional remedy based on transparency assessment is insufficient to cope with dark patterns, and it indicates that it is necessary to integrate it with other different legal remedies, functional to guarantee fair and neutral design structures and interface. After all, in the consumer

[181] Leczykiewicz, Weatherill (n 184 Ch. I), 1. Practically speaking the Authors refer to the dual vision of consumer: on one hand, as an actual person whom EU institutions have in mind when they devise regulation and, on the other hand, as a projected person who will emerge as a result of the regulatory and deregulatory efforts of these same institutions.

[182] Francisco Lupiáñez-Villanueva, Alba Boluda, Francesco Bogliancino, Giovanni Liva, Lechardoy, Lucie, Rodríguez de las Heras Ballell, Teresa, (European Commission, Directorate-General for Justice and Consumers), *Behavioural study on unfair commercial practices in the digital environment – Dark patterns and manipulative personalization: final report of the Commission study*, Publications Office of the European Union, 2022.

[183] ibid, 7.

digital market, the same concept of algorithmic opacity required to be analysed by distinguishing the technology-based opacity inherent to the design choices from relational opacity toward users.[184]

5.3 Weakness in the current fairness test

A fairness-oriented approach concerns all the regulatory policies involved in this research. Thus, as it is an overarching assessment mechanism, the fairness test is functional both for balancing the party interests and for maintaining market efficiency and welfare, and it deserves special attention to verify if and how it can allow these policies to come closer to enforcing protection against dark patterns.

In data protection law, fairness is strictly interconnected with two key principles: lawfulness and transparency. Several provisions of the GDPR (recitals 60, 71; Articles 5, 6) expressed the double nature – substantial and procedural – of the principle, and they indicate that GDPR aims at assessing the balance between different parties interest by discipline detailed, lawful, and transparent data process, by placing controllers in charge of how they comply and balance fundamental rights and interests.[185] In the light of the DMA and DSA Acts, how increased competition between intermediaries would likely shift the problem addressed from the stage of data analytics to that of data acquisition must be considered.[186]

In data protection, fairness is the mitigation of imbalances that create situations of vulnerability.

Indeed, in the context of consumer protection, the discipline of unfairness is mainly contained in the unfair terms directive and in the unfair commercial practices directive.

Based on Article 5(1) commercial practices should be prohibited if they are found to be unfair under the fairness test, which is structured through

[184] For a further discussion on algorithmic transparency matter see Mateusz Grochowski, Agnieszka Jabłonowska, Francesca Lagioia, Giovanni Sartor, 'Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory' (2021) 8(1) Premises Critical Analysis of Law 43-63; see also Erica Palmerini, 'Algoritimi e decisioni automatizzate. Tutele esistenti e line evolutive della regolazione', in Luis Efrén Rios Vega, Lucia Scaffardi, Irene Spigno (eds.), *I diritti fondamentali nell'era della* digital mass surveillance (Editoriale Scientifica, 2021) 209-244.

[185] Damian Clifford, Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 YB of Eur L 137.

[186] Laux, Wachter, Mittelstadt, Brent (n 14 Ch. II).

several layers. Generally speaking, for a practice to be considered unfair, it must amount to (a) a practice which infringes the requirements of professional diligence and may materially distort the economic behaviour of the 'average consumer' of a product or service; or (b) a practice which is likely to distort the economic behaviour of a 'vulnerable consumer'; or (c) a practice determined to be misleading or aggressive; and (d) a practice included in the blacklist of unfair commercial practices (Art. 5 UCPD).

There is a tight relationship between Article 5, Article 9, and Annex I UCPD. They form a 'three-step test' for determining if a commercial practice is unfair: (1) whether the practice appears on Annex I, the regulator will consider the practices unfair and prohibited without the need for a case-by-case assessment; (2) determine whether such practice is misleading (Arts 6 and 7) or aggressive (Art. 8) by using harassment, coercion, or undue influence (Art. 9); and (3) check whether such practice infringes the requirements of professional diligence or the trader has targeted vulnerable consumers. The practice will be considered unfair If any of these tests are satisfied.

The described legal assessment system formally applies to dark pattern clause or design, but not all trader exploitation will impair consumer judgment. In order to determine if a selling practice is aggressive under Articles 8 and 9 UCPD, the practice must impose unfair limitations on average consumer freedom of choice or conduct concerning the product or service. Again, case law played a significant role in merging the two concepts of Articles 6 and 7 on misleading and missing information and aggressive practices in Articles 8 and 9.[187] However, this combination is not without problems as it was recognized as being unacceptable considering the overall structure of the Directive. Articles 8 and 9 deal with forms of commercial practice that qualify as unlawful for reasons other than 'information deficit'. However, considering the nature of harm provoked by dark patterns, it seems unrealistic that more or better information can help the consumer make a better decision. The consumer is locked in the institutional design of data exploitation strategies. There is no way out; even if there were a way out, information is not the appropriate tool. One might argue that the consequence would be to read

[187] E.g. Case C-281/12 *Trento Sviluppo s.r.l., Centrale Adriatica Soc. coop. Arl v Autorità Garante della Concorrenza e del Mercato*, 19 December 2013 ECLI:EU:C:2013:859; and Case C-435/11, *CHS Tour Services GmbH v Team4 Travel GmbH*, 19 September 2013, ECLI:EU:C:2013:574.

deficits in digital architecture as elements that contradict the prohibition of misleading omissions.[188]

Often, the trader does not provide false or misleading information nor conceals necessary information. 'Undue influence' can be exerted by words and but by exploiting a position of power over the consumer to apply pressure.

From a different perspective, an interpretation of what constitutes an aggressive practice emerged in the case law of the ECJ, which would assist regulators and traders. It reflects the difficulties in defining aggressive practices to the extent that they are tied to human behaviour, and it is a sorely needed guidance, going beyond the phrasing of Art. 8-9 UCPD.

It has been noted that while the ECJ has contributed to clarifying the notion of fairness in the consumer law field, it has not contributed as well to defining fairness under data protection law. The GDPR in particular.[189] The merit has to be mainly attributed to soft law policy documents that investigated practical technics for implementing fairness. Indeed, the Fifth

[188] The Commission develops the argument 'Fitness Check of EU consumer law on digital fairness available at: <https://commission.europa.eu/law/law-topic/consumer-protection-law_en> accessed 1 September 2023.

[189] Case C-628/17 *Prezes Urzędu Ochrony Konkurencji i Konsumentów v Orange Polska S.A.* EU:C:2019:480. Orange Polska is a company that offers contracts to consumers for the supply of telecommunications services. Customers can amend the terms and conditions of their contracts via the online shop or by telephone. Consumers had to decide the contract terms during the amendment process when a courier of Orange Polska brought the contract to visit them. It makes some consumers feel uncomfortable to take their time to review the contract before signing it as the courier is waiting for them. In this case, the Court tackled the following question: does making the consumer take the final transactional decision in the presence of a courier' constitute an aggressive commercial practice? Options are: (1) in all cases, (2) through the exertion of undue influence where not all the standard-form contracts were sent to the consumer individually beforehand, or (3) through the exertion of undue influence where the trader, or its courier, adopts unfair conduct limiting the consumer's freedom of choice. The court held that the commercial practices at issue could not be considered aggressive in all circumstances unless they correspond to Points 24 to 31 of Annex I. According to the court, undue influence is not necessarily impermissible (such as the use of physical force); any practices that likely to significantly impair the average consumer's freedom of choice or conduct may be considered an undue influence. The consumer has not received all the standard-form contracts individually beforehand, which cannot be regarded as an aggressive practice, given that the standard-form contracts are available on the trader's website. However, certain additional norms adopted by the trader or courier in this context, such as insisting on the need to sign the contract or amendment, may constitute. Such strategies may lay in a grey area while they make consumers aware of other applied dark patterns practices.

Check individualized five evaluation criteria for fairness and promoted the construction of a 'fairness by design' involving designers while extending consumer protection duties to the design community (Ch. III).

6. The perspective of competition law

The viewpoint of competition law serves the purpose of completing the framework of reference. Incentives of intermediaries, advertisers and consumers can structurally be misaligned when revealing consumers preferences. In EU competition law, fairness has been interpreted as a reference to broad guarantees of equal economic opportunities and equal procedural treatment.[190]

Competition law presents several interconnections with consumer law and data protection law, and for this reason, it deserves better attention and efforts to be more integrated with the other disciplines. Ultimately, the market must offer consumers options for them to choose through legal tools (also market tools) designed to guarantee lawful data collection and utilisation.[191]

As a premise, digital manipulation should, in many instances, be seen as anticompetitive. However, antitrust law has typically viewed efforts to persuade consumers as forms of competition or even *pro*competitive behaviour.

The anticompetitive nature has been attributed to dark patterns by courts and scholars recognising that digital manipulation induces consumers to increase purchases, eroding user ability to act rationally. Amazon, for example, uses data about previous purchases to recommend additional purchase items to its customers.

These circumstances empower platforms to extract data and build market power. The aforementioned OECD Report 'Dark Commercial

[190] For a general overview, see: Alberto Pera, 'Fairness, Competition on the Merits and Article 102' (2022) European Competition Journal 229; Niamh Dunne, 'Fairness and the Challenge of Making Markets Work Better' (2021) 84 The Modern Law Review 230; Juliane Kokott, Daniel Dittert, 'Fairness in Competition Law and Policy' in Damien Gerard, Assimakis Komninos, Denis Waelbroeck (eds), *Fairness in EU Competition Policy: Significance and Implications. An Inquiry into the Soul and Spirit of Competition Enforcement in Europe* (Bruylant, 2020) 21.

[191] Alessia Sofia D'Amico, 'Conceptualising the interrelation between data protection regulation and competition law', in Eleni Kosta, Ronald Leenes Irene Kamara (eds.), *Research Handbook on EU data Protection Law* (Elgar, 2022) 143.

Practices' (Oct., 2022),[192] highlighted that, in addition to the impairment of autonomy, some dark patterns (e.g. drip pricing; subscription traps) could cause substantial financial loss.

A recent example is a decision of the Italian Competition Authority (AGCM) published on Feb. 23, 2023 against a company operating digital marketing services, which imposed a fine of € 300.000, finding several GDPR violations, including the use of dark patterns to obtain users' consent.[193] The company operated marketing campaigns on behalf of its clients, via text messages, emails and automated calls. Its contacts database contained data collected directly through its online portals (offering news, sweepstakes and trivia), as well as data purchased from data brokers. During the subscription process, the user was asked for specific consent relating to marketing purposes and the data sharing with third parties for marketing. If the user did not select either of the checkboxes, a banner would pop up, indicating the lack of consent and displaying a prominent consent button. The site also displayed a 'continue without accepting' option, but this was placed at the bottom of the webpage – outside of the pop-up banner – in simple text form and smaller font size, which made it less visible than the 'consent' button. The Garante, then analysed the problematic 'double opt-in', and the 'Invite a friend' options.

Thus, deceptive practices could potentially harm consumers collectively by weakening competition and sowing distrust, and could disproportionately harm specific consumers, such as less educated consumers or children.[194]

The following arguments demonstrate why antitrust law is applicable.[195]

On the one hand, information is a key element that connects competition law and data protection law: the ability to collect analyse, and disseminate personal information, represents the core of the economic

[192] OECD (2022), 'Dark commercial patterns' (OECD Publishing, Digital Economy (2022) papers No. 336 <https://doi.org/10.1787/44f5e846-en> accessed 30 December 2022.

[193] Italian DPA, order against *Ediscom S.p.A.*, [Feb. 23, 2023] <https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9870014> accessed 1 July 2023.

[194] ibid, 6.

[195] Gregory Day, Abbey Stemler, 'Are Dark Patterns Anticompetitive?' (2020) 72 Ala L Rev 1. Authors argued that the market power coercive data practices and dark patterns allow firms to accumulate negative impacts on consumer welfare by decreasing market competition. Case law with this approach is US District Court for the District of Maine - 664 F. Supp. 24 Gemini Concerts, Inc. v. Triple-A Baseball Club Assocs., 664 F. Supp. 24, 26 (D. Me. 1987) (D. Me. 1987) July 8, 1987.

value at the platform’s disposal. Data extraction and the acquisition of relevant data allow the identification of relevant insights to profile and influence users. Scholars qualify conventional privacy as a benefit of competition.

Antitrust enforcement should go further in promoting decisional privacy, and regulators should work to establish more robust interconnection between antitrust enforcement and decisional privacy.[196]

As anticipated, the ECJ has lastly ruled on the problem of the blurring of lines between competition and data protection with the (see section 4.1) decision C- 252/21 of 4 July 2023 that the Federal Cartel Office may also take into account data protection regulations in the context of antitrust decisions. The proceedings before the ECJ go back to the decision of the Federal Cartel Office in the Meta (Facebook) matter decided by the Bunderskartellamt (02/2019),[197] which prohibited Facebook data policy to

[196] At this aim, consider the observation of the OECD (n 157): ‘To the extent dominant firms use dark patterns, as discussed in Section 4, competition law relating to abuse of dominance may also be a tool through which to address them. For example, the use by a dominant firm of privacy-intrusive dark patterns to collect personal data above competitive levels could be seen as a form of exploitative conduct that may contravene laws against the abuse of dominance in jurisdictions in which exploitative conduct constitutes such an abuse (e.g. in the EU under Article 102 of the Treaty on the Functioning of the European Union and other similar national laws)’ (ibid, 32).

[197] See Bundeskartellamt, Facebook, Exploitative business terms under to Section 19(1) GWB for inadequate data processing, 6 February 2019 B6-22/16, see the case summary at <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4>. The Bundeskartellamt closely cooperated with leading data protection authorities in clarifying the data protection issues involved. In the Authority’s assessment, Facebook’s conduct represents, above all a so-called exploitative abuse. Dominant companies may not use exploitative practices to the detriment of the opposite side of the market, i.e. the consumers who use Facebook. European data protection provisions as a standard for examining exploitative abuse. This applies if the exploitative practice also impedes competitors that amass such a treasure trove of data. More specifically Facebook’s terms and conditions violate the GDPR as there is no effective consent for such extensive data processing pursuant to Article 6(1a). The problem lies in the voluntary nature of the consent, which cannot be assumed if such consent is a prerequisite for using Facebook in the first place. The problem, in other words, is that when users want to use Facebook, they do not have a choice except to accept all terms and conditions. The BKA argues that the infringement of data protection law is ‘a manifestation of Facebook’s market power’. There is a link of causality: because Facebook inappropriately processes user data, it has ‘gained a competitive edge over its competitors in an unlawful way and increased market entry barriers, which in turn secures Facebook’s market power towards end customers.’ A case summary is available at: <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4>.

collect and processing user data through Instagram, WhatsApp, Oculus, Masquerade and Instagram, combining information with the Facebook.com user accounts, without the user's consent. In practice, Bundeskartellamt prohibits Facebook from combining user data from different sources. The BKA ordered Facebook to adapt its data policies.

Meta filed a complaint against this with the Düsseldorf Higher Regional Court (OLG Düsseldorf). This submitted various questions to the ECJ in order to clarify how certain provisions of the General Data Protection Regulation (GDPR) are to be interpreted and whether the Bundeskartellamt may also take GDPR standards into account in the context of antitrust decisions.

In the case of 2019, the German Competition Authority (Bundeskartellamt or BKA) was the competent Authority because the case was qualified as a competition law case in Germany. The ECJ examined if Facebook has a dominant position in the German market for social networks. The extent to which Facebook collects, merges, and uses data in user accounts constitutes an abuse of a dominant position. Facebook's terms of service and the extent to which it collects and uses data are in violation of the European data protection rules to the detriment of users.[198]

The BKA went through the traditional steps of defining the relevant market, establishing Facebook's dominant position and laying out a theory of abuse. The BKA concludes that Facebook is in a dominant position. In specifying the exact nature of the abusive behaviour, the BKA relies heavily on the GDPR. The Court of Justice remarks that NCAs are not replacing the role of data protection supervisory authorities because they do not act within the powers and tasks conferred upon them under Articles 51(1) and 57 of the GDPR (para 49).

Be that as it may, the Court of Justice plays out with the argument of accepting the consideration of the GDPR within the broader context of antitrust and extends it into recognising that the access and the use of personal data are of great importance in the context of the digital economy, especially with regards to those business models providing their financing through the marketing of personalised advertising. Hence, the

[198] Under the new technological circumstances, tacit collusion could quickly expand beyond the classic duopoly case. The main challenge here is mainly regulatory, as most jurisdictions do not prohibit tacit collusion, considering that firms behave rationally and interdependently on the market in these instances. Gregory Day, Abbey Stemler, 'Are Dark Patterns Anticompetitive?' (2020) 72 Ala L Rev 1.

argument goes, the access to personal data and the fact that digital platforms may process that data (after collecting and linking them into large datasets) may be considered as a parameter of competition between the undertakings in the digital economy.[199]

From a different perspective, antitrust intervention could also be functional in strengthening consumer protection.[200] Competition law addresses imbalances to the detriment of consumers, albeit from a different angle compared to consumer law. In a seminal piece on consumer sovereignty, the division of labour between competition and consumer law has been described, and antitrust violations have been identified to impair the 'menu of options' available to consumers.[201]

Scholars argued that online manipulation can overcome free will and generate anticompetitive effects,[202] because they consider consumer attention the most valuable resource in platform markets to exploit information about consumer preferences for their interests.

To this purpose, design becomes the mechanism that allows platforms to catch and maintain the so-called attention cycle: designs could extend the time consumers spend on the website, expediting a sort of consumer brain dependency.[203] Anyhow, there are different levels of impact of digital architecture on consumer attention, as well as distinctive consequences: the main distinction – it must be remembered – it is between persuasion and coercion (see Chapter I).

Different jurisdictions have ruled that persuasion is inherent in competition, consequently, it does not determine infringement of antitrust law;[204] while coercion determines an anticompetitive conduct.[205] EU

[199] The opposite conclusion would disregard the reality of digital economic development and undermine competition law's effectiveness altogether (paras 50 and 51). See Alba Ribera Martínez (n 115).

[200] Damian Clifford, Inge Graef, Peggy Valcke, 'Pre-Formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections' (2019) 20 German Law Journal 679.

[201] Neil Averitt, Robert Lande, 'Consumer sovereignty' (1997) 65 Antitrust Law Journal 713-756, 714.

[202] Gregory Day, Abbey Stemler, 'Are Dark Patterns Anticompetitive?' (2020) 72 Ala L Rev 1.

[203] On the effects of digital manipulation on the human brain, see Tim Wu, *The Attention Merchants: the epic struggle to get inside our Heads* (Atlantic Book, 2017).

[204] See US case law: Sanderson v. Culligan Int'l Co., 415 F.3d 620, 623 (7th Cir. 2015). In this case, the Seventh Circuit argued that deceptive advertising should not constitute an antitrust claim because (1) advertising can be pro-competitive even if it is false, and (2) false advertising cannot preclude competition absent a coercive enforcement mechanism.

competition law preserves the function of the internal market, consequently fairness is not its focus, notwithstanding it is mentioned in Articles 101 and 102 TFUE, and it indirectly contributed to addressing uncompetitive practices.

Looking at the issue of the qualification of digital designs under the behaviours qualified as anticompetitive and punished by the antitrust authority, one can observe that, on the contrary, the same tool, the design, used fairly can play a key role for struggling anticompetitive designs.

While algorithmic transparency and algorithmic accountability principles have been discussed earlier because they need to be incorporated from the design phase of the product or application, competition policy has specific implications that are not often taken into consideration *ab origine* by the design architecture. It would be worth informing design to effective principles to struggle with the opacity and complexity of algorithms used by platforms to catch consumer preferences.

6.1 The idea of 'competition by design'

The proposal to take legal advantage of the 'competition by design' mechanism should, first, be interpreted as a suitable complement to strengthen traditional competition law enforcement in an increasingly algorithmic market reality.

The aim is not to replace the traditional legal tools because there is an inherent admission that improved competition protection could be obtained through ex-post enforcement and protection through ex-ante measures powered by algorithms. This is based on the acknowledgement that there is a relationship worth exploring between competition protection ensured to a great extent through ex-post enforcement and protection through ex ante measures powered by suitable technology.

The flexible human interpretation of norms and regulation might conflict with the rigid computer language.[206] The idea of 'competition by

For an extensive analysis, see Bruce Colbath, Nadezhda Nikonova, 'False advertising and antitrust law: sometimes the Twain should meet' (2014) CPI Antitrust Chronicle 2.

[205] A multiplicity of decisions, through different rationales, found coercion illegal as it deprives consumers of free choices and so anticompetitive. For an overview and discussion of the case law see Day, Stemler (n 40).

[206] Inevitably, there is a trade-off between the specificity and rigidity required to automate legal provisions and the benefits and needs of flexibility, and even ambiguity, of

design', as expressed by the EU Competition Commissioner – Commissioner Vestager – could respond to the exigence to ensuring algorithmic accountability in competition law. The Commissioner argued:

'[c]ompanies need to think from the start about how to use data without hurting consumers. And if they do, there's no reason why Big Data and competition should conflict'.[207]

The compliance of competition by design, as inspired by data protection regulation, would aim to ensure that competition principles are appropriately embedded into the design of the technology so that the benefits of algorithm-based markets become more readily available to consumers. If market actors increasingly conduct their business by using algorithms, 'designing in' compliance seems quite promising and could promote a forward-looking understanding of competition enforcement in algorithmic markets. Pricing algorithms, for example, need to be built in a way that does not allow collusion.

The advantages of the design tool for competition law enforcement are clear to politicians and scholars, but it is not as clear how to integrate competition policy principles into a design.

Distribution and differentiation of responsibilities for the architectural design that allow the interaction between firms and consumers via algorithms could avoid leaving the power to verify the compliance of the design with competition law principles to only a few platforms.

Specific skills must belong to those who will assume the role of implementing compliance by design: they need to be able to nudge the design of the powerful tools available to market actors in a direction that complies with well-established competition values without locking it into a specific technological paradigm. This demands an understanding of what technological developments could be more useful safeguarding good functioning market processes in the interest of consumers.

Consequently, the 'by design approach' could be effective if the designers are fully aware of the substantive competition law subject matter, the economic knowledge of anticompetitive effects, and the knowledge of

natural language because when the complexity of particularized rules increases, their formal realizability decreases.

[207] Margrethe Vestager, 'Algorithms and competition', Speech at the Bundeskartellamt 18th Conference on Competition, Berlin, 16 March 2017, available at <https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/bundeskartellamt-18th-conference-competition-berlin-16-march-2017_en.>.

technology and software development. It means that competition compliance by design can become an effective tool only if it is based on an open and constructive dialogue involving all interested stakeholders, including the enforcers, firms, computer science experts, designers and providers of algorithms, academia, and consumers.

Designers must focus on the preventive decisions that are taken and lead to a technical architecture that precludes anticompetitive behaviour. Automation, which is seeking to replicate competition law in computer code, is by far the most impactful among them. Generally speaking, preventing of illegal conduct based on implementing of self-enforcement technologies understates that law provisions can be automated. However, the extent to which law can be automated is still debated.[208]

A potential 'self-restrain' solution to control competition could consist in 'instructing' the design algorithms not to collect the categories of data that expose the firm to antitrust liability. Alternatively, even if the data was collected and processed, algorithms could be restrained in taking the consequential decision not to compete, such as not aligning to specific price variations of individual companies.[209]

From a merely technological point of view, there are also issues to solve. For example, the learning algorithms of the competition-friendly design learn from unclassified data through a trial-and-error logic. This implies choices on training data. Admittedly, algorithms could gather insights from specific available data flows that might expose the firms to competition law liability. Moreover, when it is too complex or costly to modify the algorithm learning process, the firms can introduce filters to modify the prima facie responses of the system.

Lastly, it has been observed that competition by design is unlikely to be achieved solely by focusing on automation: other design techniques should be explored to ensuring that markets work in the interest of the consumer.[210] Some of these measures lie at the crossroad between competition policy and related policy areas, in particular consumer protection and data protection.

[208] See Frank Pasquale, Glyn Cashwell, 'Four Futures of Legal Automation' (2015) 63 Ucla L Rev Discourse 26.

[209] A data flow 'self-restraint' is not new in competition policy, especially in the context of information exchanges. OECD, 'Information Exchanges Between Competitors under Competition Law: Policy Roundtable' (2010) DAF/COMP(2010)37.

[210] Giovanni Buttarelli, 'The Digital Clearinghouse gets to work', 27 May 2017, <https://edps.europa.eu/presspublications/press-news/blog/digital-clearinghouse-gets-work_en> accessed 10 June 2023.

Considering this, the EDPS proposed the establishment of a Digital Clearinghouse to bring together agencies from the areas of competition, consumer, and data protection willing to share information and discuss how better to enforce rules in the interests of the individual.[211] The Digital Clearinghouse could offer a suitable tool and framework to engage, both conceptually and practically, with other measures.

To exemplify the reason why initiatives, such as the Digital Clearinghouse, are needed, it is sufficient to think about the issue of market power in consumer law, which raises the question of whether every abuse of a dominant position violating EU competition law could also be qualified as a violation of the UCPD. As stated in recital 8 of the UCPD, it indirectly protects fair competition and abuse of dominance for 'conduct which is directly exploitative of consumers.[212] Consequently, the concept of market power can be incorporated into an assessment of a UCPD violation, even if not every monopolist, or market actor with significant market power, breaches the UCPD. Vice versa, not every exploitation of consumer irrationality violates the UCPD.

Dominant market actors that exploit of consumer cognitive errors should be under stricter assessments of EU consumer law, particularly in digital markets. The special regimes the proposed DMA and DSA envisage for digital platforms show that the European Commission tend to reflect on their market power outside of the 'competition law box'. From a substantial point of view, the design must reproduce all of these interconnected protections, including competition requirements.

[211] On 14 March 2017 the European Parliament adopted a resolution on 'fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement' which included a call for «closer cooperation and coherence between different regulators and endorsed the establishment and further development of the Digital Clearinghouse as a voluntary network of enforcement bodies can contribute to enhancing their work and their respective enforcement activities and can help deepen the synergies and the safeguarding of the rights and interests of individuals». More information is available at <https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en>.

[212] Commission, 'Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings' [2009] O.J. C 45/7, para 7.

6.2 Anticompetitive dark patterns

Theoretically, a dominant firm could abuse its power by lowering the privacy and data protection it offers consumers. The free movement of data is, in fact, a new fundamental freedom in a data-driven economy and the result of a dynamic check and balance between different interests and principles, all belonging to the crossroad area under examination.[213]

For this reason, the refusal of companies to grant access to data and the adoption of non-transparent contractual conditions for the data-policy could arguably constitute an exploitative abuse in some jurisdictions.[214] Competition Authorities in different countries have recently issued significant cases of dark commercial practices.

One of the first European Competition Authority to intervene was the Italian Antitrust Authority (AGCM), which fined Facebook € 10 million in late 2018, recognizing that the famous social network had engaged in unfair business data practices breaching the Italian Consumer Code implemented the UCPD.[215]

The conduct detected by the AGCM concerned the claim by which Facebook induced users to register on its platform: 'it's free and it will be free forever'.

The Antitrust sanction was later revised by the Regional Administrative Tribunal (in short: T.A.R.) Lazio, with the ruling on December 18, 2019.[216] T.A.R. Lazio upheld the AGCM's sanction on the point, stating that

[213] Fazio Emanuele, 'Il problema delle competenze settoriali e l'adozione di un approccio olistico dalla data-driven economy' (2020) 66(3) Il diritto dell'economia 653-678.

[214] Anna Barker, 'Consumer data and competition: A new balancing act for online markets?', OECD Going Digital Toolkit Notes, OECD Publishing, No 5, 2021) <https://doi.org/10.1787/e22e3a47-en> accessed 22 November 2022.

[215] The first decision taken by the AGCM was in 2016, when the Authority fined online dating site Edates EUR 350 000 for breach of the Art. 21 and 22 Italian Consumer Code (d.l.vo n. 206/2005) upon finding that, following a free registration to the site or a two-week trial subscription offered at a low price, consumers unknowingly found themselves bound to a six-month premium subscription at a cost of EUR 19 a week.

[216] Jan. 10, 2020, Nos. 260 and 261. Tar Lazio, sez. I, 10 gennaio 2020, n. 260 published in Diritto & Giustizia 2020 (13 gennaio), and commented by: Antonio Leo Tarasco, Michele Giaccaglia, 'Facebook è gratis? "Mercato" dei dati personali e giudice amministrativo' (2020) 66(102) Il diritto dell'economia 263-301. While, Tar Lazio 10 gennaio 2020, n. 261 commented by Gian Luca Pastuglia, 'Prime note in materia di coordinamento tra disciplina delle pratiche commerciali scorrette e regole privacy' (2021) 6 Dir Industriale 511.

Facebook should have informed the user that by activating an account, they would have to submit their personal data for commercial purposes.

According to the T.A.R., the social network was obliged to comply with clarity, completeness and non-misleading information principles provided by consumer law.[217] In particular, the AGCM stresses that the information was expressed with complex and detailed technical specifications and indications were unclear, fragmented into different sections, and without adequate evidence of the commercial use of the data. Insights were not immediately accessible, without any evidence in favour of the consumer, who could not, therefore, use of a comprehensive and easily accessible unitary information framework. In this case, a so-called layered information was used: it is obtained according to the layering technique, widely employed on the web, which consists of dividing information into different levels so that it is easier for the user to understand.

The Authority considered that Facebook exerted undue influence on registered consumers by pre-selection of the broadest consent to data sharing by placing restrictions on the use of the website when consumers decided to limit their consent to dissuade them from doing so.

It is interesting to note the differences between the mentioned Italian decision and the decision of the Higher Regional Court of Düsseldorf (Oberlandesgericht) on the case *Facebook v. Bunderskartellamt* of August 26, 2019,[218] which rejected the appealed decision for lack of competence. While the AGCM proceeded against Facebook on the assumption of a violation of consumer law, as the Authority has both competencies in the field of consumer law and in that of competition law, the Bunderskartellamt is exclusively competent for antitrust law (specifically for the violation of the section 19 and 32 of German Competition Act, the GWB).[219] Notwithstanding the critics, the German Authority was able to rule the case, under competition and antitrust law, while civil Courts are competent for unfair commercial practices.

Firstly, the BKA greatly justifies its reliance on the GDPR to establish a competition law infringement.

[217] Otherwise, the second Antitrust sanction was annulled by the T.A.R. Lazio. This one concerned the 'undue conditioning' of users whose data are transmitted to third parties without their consent. Indeed, the T.A.R. held that users are given a choice whether or not to allow integration between different platforms. On this second aspect, however, many concerns remain.

[218] Higher Regional Court of Düsseldorf (Oberlandesgericht Düsseldorf), *Facebook v. Bunderskartellamt*, 26 August 2019, [2019] D'Kart Antitrust Blog, Case VI-Kart 1/19, OLG.

[219] See section 6.

Instead of focusing on the Commission's position,[220] the Bundeskartellamt relies on the case law of the German Federal Court of Justice, which considers contract terms abusive if they violate the German Civil Code (in particular when a party with superior power imposes such terms). By analogy, the BKA holds that 'the European data protection regulations must be considered when assessing whether data processing terms are appropriate under competition law.' As the GDPR does not aspire to complete consistency of enforcement, competition authorities can also consider and interpret its provisions within the specific assessment to assert that the access and the capacity to process are relevant to the competitive dynamics, as clarified by the ECJ ruling of 4 July 2023.

Contrary to the Bunderskartellamt's assertation, the Oberlandesgericht argued that Facebook's data policy does not cause any competition damages. There were no exploitative practices which damaged users, nor any exclusionary effects for competitive social network.

Later, with the decision of 23 June 2020, the antitrust division of the Federal Court of Justice decided that the Bundeskartellamt's prohibition could be enforced.[221] There were no severe doubts as to Facebook's dominant position in the German market for social networks nor can it be doubted that Facebook abuses this dominant position by using the terms of service prohibited by the Bundeskartellamt:

'the lack of options available to Facebook users does not only affect their personal autonomy and the exercise of their right to informational self-determination also protected by the GDPR. In light of the considerable barriers existing for network users who would like to switch providers ('lock-in effects'), this lack of options also exploits users in a manner which is relevant under competition law, since due to Facebook's dominant position, the user is no longer able to effectively exercise its controlling function. According to the Bundeskartellamt's findings, a considerable number of private Facebook users wish to disclose less personal data. If competition on the market for social networks were

[220] 'any privacy-related concerns […] do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules.'

[221] KVR 69/19 - Beschluss vom 23. Juni 2020. Courtesy translation of Press Release No 080/2020 published by the Bundesgerichtshof (Federal Court of Justice) on 23/06/2020 provided by the Bundeskartellamt, available at <https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html.> accessed 21 January 2023.

effective, this option could be expected to be available. Users who consider the scope of the data disclosure to be a key criterion in their decision could switch to other alternatives. The terms of service structured in this way could also impede competition'.[222]

As far as the relation between data protection law and competition law is concerned, significant are the seven questions the Higher Regional Court of Düsseldorf asked the ECJ, one concerned: (i) the competence of a national competition authority to assess a company's compliance with the GDPR. According to Advocate General Rantos, while exercising the conferred powers a national competition authority, such as the BKA, law may have considered whether the conduct being investigated is compliant with other regulations, such as the GDPR. This is possible if the competition authority: (i) is carrying out the examination incidentally and therefore without prejudice to the interpretation and the enforcement of the GDPR by the competent data protection authority; (ii) is adopting the interpretation given by the competent supervisory authority and complying with any ruling it has issued with regard to the same/similar conducts; (iii) informs and cooperates with the competent supervisory authority where that authority has begun or is about to begin an investigation of the same practice.

Meta Platforms appealed the decision issued by the BKA before the Higher Regional Court of Düsseldorf, which stayed the proceeding and referred a request for a preliminary ruling to the European Court of Justice which conducted to the widely mentioned decision of 4 July 2023.[223]

The whole case is part of the broader debate about the role played by competition law, consumer law and data protection law in digital markets due to the overlapping scope of their application, as in the case of services offered by digital platforms.[224]

[222] ibid

[223] Case C-252/21, *Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd.*, Facebook Deutschland GmbH v Bundeskartellamt, Opinion of Advocate General Rantos (2022).

[224] Oberlandesgericht Düsseldorf, Request for a Preliminary Ruling, 22 April 2021, in *eur-lex.europa.eu*. See more comments in Claudia Martorelli, 'AG Opinion in Case C-252/21: The interplay between Data Protection Law and Competition Law' (15 February 2023) MediaLaws available at <https://www.medialaws.eu/ag-opinion-on-case-c-252-21-the-interplay-between-data-protection-law-and-competition-law/#_ftnref7> accessed 20 July 2023.

7. Preliminary conclusions

European legal framework aims at counteracting manipulative designs, such as dark patterns, which have been evolving quickly. The frame still underlines the persistent difficulties for legal systems to protect genuine will when these techniques push consumers toward choices that exclusively benefit the provider at the expense of their autonomy.

Firstly, the absence of a general tort for 'exploitation of cognitive biases' should be acknowledged.[225] This lack could also originate from the dynamic nature of dark patterns which continuously emerge under new shapes: an overarching shift moves manipulative designs with a narrow focus on static user interfaces, towards the inclusion of dynamic designs, relying on data-driven algorithms, which interfere with individual decisions in subtler ways. Also, a dividing line emerges between information/advertising-based commercial practices on one side and non-information based commercial practices on the other side. This line needs to be upheld.

Chapter II has shown that the nature of remedies involved is surfacing at the crossroads between consumer, data protection, and competition policies. Particularly, GDPR and UCPD offer provisions indirectly addressing consumers' manipulation and relating to digital architecture design. Only recently legal scholars have started to specifically focus on the possible ways to coordinate the intricate legal framework of AI-powered technologies.[226]

The need for a pluralistic approach to protect consumer autonomy comes up to mix the strengths of one regime, compensating for the weaknesses of the other.

Consumer law and data protection law are not yet a perfect match, and better coordination is suitable to improve digital consumer autonomy protection: in consumer law, the flexibility of the fairness test could, for example, implement safeguards against the practice of using consent to legitimise data collection and processing as a condition for the transaction decision. Moreover, under the UCPD, a breach of the general prohibition

[225] Cass R. Sunstein, Fifty shades of manipulation (2016) Journal of Marketing Behavior 213-244.

[226] Artur Bogucki, Alex Engler, Clément Perarnaud, Andrea Renda, 'The AI Act and emerging EU digital acquis. Overlaps, gaps, and inconsistencies', CEPS-In-Depth Analysis (2022) available at <*www.ceps.eu/ceps-publications/the-ai-act-and-emerging-eu-digital-acquis/*> accessed 10 August 2023; and Cristina Poncibò, 'Artificial Intelligence Platforms: Safeguarding Consumer Rights in the EU' in Larry Di Matteo, Geraint Howells, Cristina Poncibò (eds), Artificial Intelligence and Consumer Law: Comparative Perspectives (CUP forthcoming 2024).

of unfair commercial practices (Article 5), the prohibition of misleading (Articles 6-7 UCPD) or aggressive practices (Articles 8-9 UCP Directive) play a role against deceptive designs, as well as, a breach of determinate practices of the UCPD blacklist (Annex I, especially points 5, 6, 7, 18, 19, 31, 20 and 26). Numerous examples can be found in the Commission's Guidelines on the interpretation and application of the UCPD:[227] differently visible buttons, trick questions, misleading free samples and subscription traps, or 'confirmshaming'.

On the other side, data protection law can inform the interpretation and development of consumer law and thereby help to adjust consumer practices to the demanding modern economy, where personal data processing plays a significant role, as well as through the digital architecture design.

Indeed, dark patterns might constitute a breach of consent and transparency under GDPR, or they can also constitute a violation of the principle of privacy by design (Article 25 GDPR). Several examples can be found in the EDSA's Guidelines 3/2022 on 'Dark patterns in social media platform interfaces' of March 14, 2022.

Lastly, competition law is also relevant, for the analysis's specific purpose: in digital market the line between the various forms of consumer harms and market failures blur. The enforcement perspective emphasized, as well, the fact that in the digital market, harms prevented by different authorities are inextricably interlinked.

The suitable way to eliminate unfair design patterns in e-commerce, social media, and other user web interfaces is still an open question. Currently, European and National legislators continue to generate new regulations. The most evident steps are DSA and DMA regulations, which implement *ad hoc* provisions on dark patterns.

For example, the DMA opens the door to requiring huge companies to, at least, acknowledge the risks choice architectures pose to their customers, increasing the quality of the relationship with consumers through a better communication process.

As distinctive scholars recently underlined it, incongruences also exist in new regulation itself. There is no reason why a particular practice should not be able to violate several laws and consequently be sanctioned under

[227] Commission (Notice), 'Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and the Council concerning unfair business-to-consumer commercial practices in the internal market' [2021] OJ C 526/1.

several regimes.[228] As this chapter has demonstrated, one of the problems that arises in determining whether the DSA will be applied with priority on the regulatory patchwork already applicable to dark patterns.

UCPD and the GDPR take precedence over the DSA (Article 25 (2) DSA), which ultimately fails to establish a clear scope of applicability and make the concrete regulation of dark patterns dependent on EU guidelines. However, even soft law, particularly guidelines, present weaknesses: they require quite a long time to be issued, and there is a risk that those guidelines will mainly address specific dark patterns – like those already listed in Article 25, section 3 – rather than providing an exhaustive solution addressing the actual diversity of dark patterns. For now, interface designers will have to rely on the existing guidance under the UCPD and the GDPR. It has also been argued that the effect of the DSA in this context will depend on the interpretation of the former legislations: it cannot be ruled out that the DSA will affect the interpretation of the UCPD and the GDPR, but it does not seem to have been the intention.[229] Dark patterns concerning commercial practices can be addressed by DSA when they do not affect the consumers' economic interests (e.g. 'taste and decency'), also including privacy aspects. On the side of privacy, DSA may apply when consumers decisions concern non-personal data.[230]

Criticalities are still numerous. For example, it must be discussed whether and to what extent fairness of choice architecture is protected by the GDPR and, ultimately, the nature of such fairness. Consumer agencies and organizations play a significant role in defining legal standards. Perhaps this will change with the new Directive on Representative Actions, where the GDPR forms part of the list of consumer legislation that qualified entities can enforce.[231]

For all these reasons and concerns on peculiarities of data-subject/consumer cognitive vulnerabilities, this chapter has investigated the available rules applicable to choice architectures, individualising the dual basis around which they are developed: transparency and fairness.

Lawful design will combine them. A step forward was made by DSA, although with the expressed concerns.

[228] ELI (drafters: Marie Jull Sørensen, Peter Rott and Karin Sein), Response (n 11; 160).

[229] Trzaskowski (n 51 Ch. I) 31.

[230] ibid

[231] BEUC (n 141) 47.

The analysis underlined the coordination problems between the policies is, primarily, taken on the role of case law, which implicitly or explicitly contributes to assessing the lawfulness of data exploitation strategies. European Court has emphasised that transparency requirement implies that consumers must be able to evaluate the economic consequences of a term or a contract. Transparency is not viewed solely as a procedural control related to the drafting of clear and intelligible contract terms. However, it involves a requirement to effectively inform the consumer of the contract terms and their implications.

Furthermore, adequate protection of genuine autonomy is also troubling because most binding provisions are based on traditional concepts, which do not include the novel characteristics of the exploitation of cognitive bias. The analysis has revealed severe deficiencies in the proper handling of emerging consumer vulnerabilities, mainly because the legal system is not designed for them, being mostly based on consumer cognitive bias. Due to this gap, discrepancy exists between the purposes of regulations in force and their real impact.

A move beyond a narrow legal dark pattern counter-strategy could be achieved, setting incentives for website providers to implement bright interface design features voluntarily.

In this respect, with Chapter II, the practical importance of the 'by design approach' surfaced: based on preventive legal thinking, considering the necessity of setting up provisions, norms and principles with an interdisciplinary approach, technology plays an essential role in simplifying and presenting legal rules leading consumers towards a fair legal process through bright patterns.

The preliminary achievements lead to further analyse: (i) the suitable legal model because new interpretations of the law alongside data-driven technologies developments generate unique effects and create different power relationships between stakeholders, which should be considered when an efficient and comprehensive regulation is setting up; (ii) the constraints with traditional legal notions upon which current regulation are based, such as average digital consumer, fairness, trader, vulnerabilities. They do not appear sufficiently ponder fundamental lessons regarding behavioural economy and cognitive sciences contributions.

Following this line of priorities, Chapter III develops the reasoning towards the purposeful analytical insights to improve the coherence of the legal protection for genuine autonomy with the pragmatical challenges of the digital architecture.

III

REDESIGNING TAXONOMIES AND LEGAL MODELS OF EU PRIVATE LAW TO PROTECT THE RIGHT OF AUTONOMY IN THE DIGITAL ENVIRONMENT

1. Arising protection exigencies for autonomy: a review

Drawing together the previous findings, this opening chapter outlines the emerging directions along which adequate consumer autonomy protection must be orientated.

Essential outcomes are, firstly, drawn as follows.

Chapter I has described the general challenges of data-driven technologies, emphasising the significant contribution of behavioural studies in grasping the novel nature of consumer vulnerabilities, which required setting up the analysis on consumer autonomy in the light of the evolving Law 3.0 way of reasoning.

Chapter II focused on the analysis of the case-study of dark patterns, describing the complex frame of applicable provisions belonging to data protection law, consumer law, and competition law, specifically concerning transparency and fairness. These two principles must be interconnected to protect consumer autonomy in digital market. Furthermore, chapter II emphasised the fast-evolving types of dark patterns, which predominantly bring together the exploitation of emotional and cognitive digital consumer vulnerabilities. The criticalities posed by dark patterns underlined that the 'quantity' of information required by the traditional information approach is no longer the decisive element; instead 'quality' of information related to informational visualisation and representation (design) is essential and often decisive, for social changes and individual determination.

Chapter II also described how law in practice, through cases and guidance, has already emphasized the need to go beyond a safe policy field to protect digital consumer autonomy.

Having collected these results, Chapter III projects the main findings toward suitable approaches, models of law and research methods, specifically concentrating on the importance of regulation by design. In this respect, this last step is intended to be in line with the most recent research in European Private law which 'despite its growth, [EU private law] has remained 'fragmented', unsystematic and in part even contradictory in terms of its terminology and values. These structural problems are still evident in recent EU legislation and are unlikely to be remedied in the foreseeable future. For future development, it remains therefore necessary to consider whether and in what way the 'acquis research' can be helpful to strengthen the coherency of the EU private law by elaborating overarching concepts, principles, and structures and how it should be further developed with regard to the new challenges'.[1]

With this purpose, Chapter III sketches out the following three primary legal shifts to approaching the effective protection of autonomy suitable.

First, section 2 considers why and how to implement the fragmentary legal framework applicable in light of the European Authority debate.

Secondly, section 3, concerning the lessons of dark patterns, points out why and how data-driven technologies determine the obsolescence of traditional categories. This second research branch will not only emphasize the evolution and new content that traditional legal notions have acquired but also introduce insights to approach the changing face of weaknesses and protection in EU private law. In particular, vulnerabilities and average consumer are analysed in depth because of their crucial roles in determining the key elements influencing authentic consumer self-determination.

Thirdly, section 4 considers how a suitable regulatory model is required to implement through concrete techno-legal standards and design interfaces for a 'user-centric' model, where autonomy is designed ex ante, and with keen attention to the quality of data and the process of algorithmic training. In this way, it will emerge the contributions of other sciences, such as behavioural sciences, to effective implementation and accountable regulation of authentic autonomy protection.[2]

[1] André Janssen, Matthias Lehmann, Reiner Schulze, 'The Future of European Private Law – An Introduction' in André Janssen, Matthias Lehmann, Reiner Schulze (eds.), *The Future of European Private Law* (Nomos 2023) 35.

[2] See Roger Brownsword, Eloise Scotford, Karen Yeung (eds.), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press 2017). Ultimately, refer also to the programme of the conference on 'Digital Vulnerability in European Private Law', at the

2. New directions to coordinate a fragmented regulatory program

As previously emerged, the need to implement coordination between regulations triggers the need to go beyond a single policy, identify proper regulatory instruments to protect autonomy when challenged by dark patterns. European private law is characterized by the strategic coordination of sectorial and horizontal regulations.

Therefore, apart from specific prohibitive provisions of dark patterns, data protection law, consumer law and competition law, where information has a predominant profile, have all been shown to be, directly and indirectly, functional to protecting the right to autonomy in the digital environment.

For example, one of the areas in which dark patterns are discussed more is that of the pre-ticked consent box or consent to cookies, consequently, data protection law acquired a crucial importance (Ch. II).

Briefly, the GDPR is a comprehensive law that supports other regulations. Unlike the previous data protection law (Data Protection Directive 95/46, and in the e-Privacy Directive), GDPR contains an evolved concept of consent: a primary legal tool to protect user self-determination. Further clarification and specification of the requirements for obtaining consent, pragmatically compliant with regulation, was added with the Guidelines on consent under Regulation 2016/679,[3] adopted on 10 April 2018 by the WP29 and the Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020 by the Edpb.

The jurisprudential interpretation over the years has always contributed to individualizing remedies for harms caused by effective will and substantial consent. The interpretative function, exercised by judges, recently remarked on rationales better coordinate different policies to protect values and rights belonging to a data scientist. This is clear in the ECJ C- 252/21 decision of the Facebook/Meta proceeding, which brought the interface between antitrust and rules on data protection to the international debate.[4]

Law Department of the University of Ferrara, organized by Prof. Alberto De Franceschi on 15 and 16 June 2023.

[3] EDPB (n 80 Ch. II), accessed 10 June 2022.

[4] It was already clear in the German Facebook case decided by the Bunderskartellamt: case B6-22/16 Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing available at <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-2216.html?nn=3600108>.

Considering the changeable nature of dark patterns, an intrinsic limit of GDPR familiar to many other Regulations, it is the fact that it is not based on earlier empirical studies on consumer behaviour when consent is given in a data-driven technological context.[5] This could be a crucial impediment in order to protect consent under dark patterns pressure, as these digital designs exploit cognitive and emotional human resources.

The horizontal EU consumer law acquis shows that many consumer Regulations can address misleading and unfair design. Like data protection law, consumer law is aimed at strengthening consumer rights, with specific attention to their ability to make informed decisions. Nevertheless, as previously affirmed, even if the New Deal for Consumers adopted by the European Commission in 2020 contributed to modernizing the context and to improving the enforcement tools – for example, with the representative actions for the collective interest of consumers – for the new features of the market, the efficiency of the informational approach is limited with regards to data-driven technological applications.[6]

Steps forward have been taken. In general, it has been observed that European Authorities intervene with specific provisions for dark patterns (e.g. DSA) because the existing regulation, such as GDPR, cannot include the multitudes of different tactics. They can't fall under the unique umbrella concept but truly impact in different ways and cause several types of harm to the data-subject/consumer consent.

Likewise, the relationship between consumer law and data protection law, and even between data protection law and competition law, is identified as a cooperative interrelation, considering:

'consumers are also data subjects, whose welfare may be at risk where freedom of choice and control over one's personal information is restricted by a dominant undertaking'.[7]

The 'integrationist approach' accepts the incorporation of privacy arguments into the competition law framework. The GDPR, the UCPD and the UCTD should be understood as laying down a common fairness

[5] Lucilla Gatt, Roberta Montanari, Ilaria A. Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' (2017) 2 Politica del Diritto 343-360.

[6] Parliament, Council Directive (EU) 2020/1828 of the of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L 409, 1-27.

[7] EDPS, 'Preliminary Opinion of the European Data Protection Supervisor. Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy' (2014) 33.

field at both substantive and enforcement levels. All three legislative measures can be broken down into requirements on standardization and individualisation of legal relations. This holistic perspective allows for finding commonalities and for a mutual transfer of the rights of consumers whilst respecting the particularities of each legislative measure.

As this research highlights, the coordination of different regulations and domains do not only offers positive insights but also problematic issues to resolve, mainly focused on how to achieve a suitable correlation.

Gaps and overlapping rules are frequent. For example, DSA allocate responsibilities only with reference to non-commercial practices, leaving aside all the other potential data-control actors. Alternatively, GDPR is often integrated by soft law, which, pragmatically contributes to increasing legal compliance when concerns about the homogeneous application of rules arise.

Institutional debate was recently widely spread towards these problems, in the wake of the European Commission is proposal of a New Consumer Agenda (2020), which aims to analyse whether additional legislation or other actions are needed in the medium term to ensure equal fairness online and offline.[8]

With the subsequent EU Fitness Check on digital fairness (2022), the Commission wished to concretely determine whether the existing key horizontal consumer law instruments remain adequate for ensuring high consumer protection in the digital environment. The Check has a general nature, as the provided program will cover five main evaluation criteria: effectiveness (fulfilling expectations and meeting its objectives); efficiency (cost-effectiveness and proportionality of actual costs to benefits); relevance (to current and emerging needs); coherence (internal and external with other EU interventions or international agreements); and EU added value (producing results beyond what would have been achieved by Member States acting alone). Depending on the results, the follow-up outcome of the Fitness Check could take the form of a new legislative proposal, an improved implementation through better enforcement and guidance, or further monitoring.[9]

[8] Commission, 'Communication to the European Parliament and the Council New Consumer Agenda on Strengthening consumer resilience for sustainable recovery' COM(2020) 696 final.

[9] Commission, 'Fitness Check of EU consumer law on digital fairness' (2022) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en> accessed 28 December 2022.

During the second Annual Digital Consumer Conference held on 21 November 2022, the European Commission announced that the event was dedicated to investigating the digital aspects of consumer policy. Specifically, the central theme was 'ensuring fairness and safety for consumers in the digital world', where stakeholders underlined the necessity to reflect on whether the existing EU legal framework is still fit for purpose. Several panellists answered negatively, considering consumer law not sufficiently fit to tackle digital asymmetry, which is a structural state of power imbalance between consumers and traders (that, notably, have access to consumer data).

One panellist called for putting forward a 'Digital Fairness Act' that would tackle the issues hitherto not satisfactory manner addressed by recent legislation.

Several panellists underlined the importance of taking a holistic approach, both when assessing the legislative framework (notably how consumer law interplays with data protection, competition law, the Digital Services Act, Digital Markets Act, AI Act etc.), but also concerning the enforcement.[10]

With specific regard to dark patterns, uncertainty exists about the interplay of UCPD and DSA, and there are concerns about the grey areas in which many designs could be placed. This is the reason why it is doubtful if they can be assessed by the UCPD fairness test. This situation 'has a massive chilling effect [of legal uncertainty] on the enforcement of the law, as there is a great risk of having to bear litigation costs, including the costs of the defendant'.[11]

Insights come from the intent to increase the effectiveness of consumer protection.

Precisely, stakeholders proposed to introduce the reversal of the burden of proof; a new duty of care to ensure fairness by design; and the further addressing of personalisation practices, including targeted advertising that amounts to commercial surveillance and personalized pricing, the prohibition of dark patterns, and the protection of minors. Notably, the

[10] The enforcement power differs depending on authorities – like the Italian Competition Authority – have powers in several areas of law, such as consumer and competition law <https://commission.europa.eu/system/files/2023-03/Report%20ADCE22%20final.pdf>.

[11] ELI (drafters: Marie Jull Sørensen, Peter Rott and Karin Sein), Response of the European Law Institute on European Commission's Public Consultation on Digital Fairness – Fitness Check on EU Consumer Law (2023) <https://www.europeanlawinstitute.eu/> accessed 3 May 2023.

proposal relating to the reversal of burden of proof deserves attention: data exploitation strategies structurally disadvantage the consumer and can potentially infringe consumer rights. Data exploitation strategies in light of the broader legal architecture, remind to contract law, where business organisations elaborate standard terms before concluding a contract and impose them on consumers, whose only choice is between 'take it or leave it'. Negotiations on pre-formulated standard terms are the exception to the rule, that was why Directive 93/13/EEC Article 3 (3) has shifted the burden of proof for the existence of preformulated contract terms to the supplier. This kind of reasoning can be transferred to data exploitation strategies.[12]

The profile of enforcement has also been widely debated. European competencies in the enforcement area are limited. However, the proposed Enforcement Package, part of the New Deal for consumers, will improve it, attributing more power to the European Commission, such as power for investigations.

It was also noted by the panel that 'as regards private enforcement, the artificial intelligence Act does not, at the moment, include the possibility of collective redress through the Representative Actions Directive and therefore, in a mass harm situation caused by an AI system, consumers may not have a right to seek collective redress'. Indeed, some other participants had a different view, promoting the need for public enforcers to acquire more investigation powers, such as unannounced inspections and IT tools to effectively detect, monitor and sanction unfair practices.

In the wake of this institutional debate, academics also developed their analysis towards the needed equal fairness online and new criticalities that the digital consumer must face. In particular, the initiative of the European Law Institute (ELI) should be mentioned: the Institute mandated

[12] Rationalisation serves as the standard argument to justify and to legitimate pre-formulation for a particular business or even for a whole industry. Data exploitation strategies pursue precisely this objective. Providers are neither willing nor able to negotiate with the consumer individually as to which data should be collected for what purposes. Pre-formulated options do not undermine the standardising character. The options offered are equally pre-designed and pre-formulated. They form an integral part of the technological infrastructure and should not be understood as a form of negotiation. In Germany, consumer organisations have successfully brought to court companies that started to use different default settings in standard terms to insinuate individuality. So far, the CJEU has not dealt with default settings in data exploitation strategies as a form of commercial practice. However, the CJEU confirmed that the Directive covers default settings. If, and if so under what conditions, data exploitation strategies allow for a reversal of the burden of proof remains to be discussed.

academics to respond to the Commission's public consultation – a questionnaire – focusing their attention on potential suggestions to improve EU consumer law for the benefit of consumers.

On 20 February 2023, ELI submitted the response to the Commission,[13] which was also publicly presented and discussed during the webinar on 27 April 2023.[14]

The proliferation of dialogue between stakeholders reveals the intent to set up a co-regulation process, based on interdisciplinary participation, to develop a standard set of criteria. The primary intent will be not to apply to the digital economy and society legal rules without seriously by analogy considering the role and function of organizations from civil society.

3. The disruption of traditional legal concepts

The start of the discussion about the impact of (technological) design on legal concepts implied in this analysis lays down a widespread consideration: the traditional distinction between average and vulnerable consumers, rooted in consumer law, no longer holds up. This could be read as well as a corollary of the expansion of the European contract law, which initiated a profound change in structures and principles that distinguishes European contract law in the transition to the digital age from the first phase of its development.[15]

Following this line of reasoning, among other things, the discussion toward the traditional legal 'coordinates of references' surfaces again: by way of example, scholars have already recognised the problematic connection between the assessment of transparency and the identification of the proper legal benchmark, which it might not be the (UCPD) average consumer.[16]

[13] Refer to the website: <https://www.europeanlawinstitute.eu/news-events/news-contd/news/eli-submits-a-response-to-the-european-commissions-public-consultation-on-digital-fairness/>.

[14] Webinar on ELI Response to the European Commission Public Consultation on Digital Fairness will begin in 1 day on Apr 27, 2023 <https://www.europeanlawinstitute.eu/>.

[15] It was observed by Reiner Schulze, 'European Private Law in the Digital Age – Developments, Challenges and Prospects', in Janssen, Lehmann, Schulze (n 70 Ch. III), 153.

[16] For an attentive discussion on the point: Fabrizio Esposito, Mateusz Grochowski, 'The Consumer Benchmark, Vulnerability, and the Contract Terms

Empirical findings show that the level of awareness does not determine the capability to resist dark patterns[17], which are devoted to exploiting cognitive bias. Consequently, protecting the right to autonomy needs to be reconsidered in light of the evolution of traditional legal concepts and premises.

Referring to the following subsections, this introduction towards two of the central concepts for the research (section 3.1, and 3.2) – vulnerability and average consumer – aims to contextualize the specific need to review them within the more general narrative of the disrupting effect of technologies.

Nonetheless, the awareness that a multiplicity of academic approaches exists when considering the impact of digital technology on traditional legal concepts: some are based on the symbolic 'law of the horses' debate,[18] some others are more moderate, contemplating only the need of adaptation.[19] Thus, two premises must be settled when reviewing traditional concepts and categories.

From a functional point of view, when the object of investigation is techno-scientific, the relationship between socio-legal and scientific paradigms can reveal the tension within a wider understanding of the phenomena, which calls for different disciplinary tools, even integrating law into the cultural context.[20]

Transparency: A Plea for Reconsideration' (2022) European Review of Contract Law 18(1) 1-31; and Max Planck Private Law Research Paper (2022) No. 22/11, <SSRN: https://ssrn.com/abstract=4109474> accessed 1 June 2023.

[17] Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet *et al.*, 'I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous! - Dark Patterns from the End-User Perspective' (2021) Designing Interactive Systems Conference 763.

[18] The intellectual clash between Easterbrook and Lessig can be summarized as follows: the first, at the opening of a conference, assimilated, provocatively, cyberlaw to a right of horses to indicate the uselessness of horses; while the second offered, subsequently, the opposite perspective, see Frank Easterbrook, 'Cyberspace and the Law of the Horse' (1996) U Chi Legal F 207-216. Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harv L Rev 501.

[19] Lidia Bennett Moses, 'Adapting the Law to Technological change: a comparison of Common Law and Legislation' (2003) 26 UNSWLJ 394; Colin Tapper, 'Judicial Attitudes, Aptitudes and Abilities in the Field of High Technology' (1989) 03(4) Monash ULR 219.

[20] Stefano Rodotà, 'Diritto, scienza, tecnologia: modelli e scelte di regolamentazione' (2004) 3 Riv crit dir priv 357. It has also been noted that «in the field of the humanities, comparative analysis plays a substitution function for the 'experimental' analysis that characterizes the natural sciences». See Gianmaria Ajani, Domenico Francavilla, Barbara Pasa (eds), *Diritto comparato. Lezioni e materiali* (Giappichelli 2018) 5.

Apart from the increasingly urgent need for an interdisciplinary approach and the consequent use of different methods of analysis, such as quantitative and empirical ones (section 4.2),[21] it is also necessary to observe the complex nature of legal matters, as an endemic feature of the object of study. The adjective complex must be considered as a 'scientific parameter', where instead of the traditional predictable standards, unpredictability and inhomogeneity become common references to explain real phenomena.[22]

A complex, or adaptive system comprises a plurality of interconnected and interdependent elements whose dynamics are based on models and experimental representative patterns. Blockchain is an example. Methods based on computer simulations are required to analyse these systems. It is the so-called agent-based model: a computational model that identifies the components (individual, collective, organisations or groups) and assigns each of the technical parameters, according to which managing the interactions between the variables and translate, thus, information into numbers. Rationales governing the functioning of technologies are heterogeneous because they inform different, sophisticated, agent-based models.[23] Recently, agent-based systems have been applied to humanities. Economics has been a pioneer domain in this field, as it is an example of a complex system: although it functions through recurring logic, it evolves unpredictably.[24]

[21] About the methodological pluralism see: Roberto Scarciglia, 'Strutturalismo, formanti legali e diritto pubblico comparato' (2017) 3 DPCE 649; Pier Giuseppe Monateri, Rodolfo Sacco, 'Legal Formants' in J. Eatwell *et al.* (ed.), *The New Palgrave Dictionary of Economics and the Law* (2, Macmillan 1998) 531-533; Leontin Jean Costantinesco, *Il metodo comparativo* (Giappichelli 2000).

[22] Pier Giuseppe Monateri, 'Deep inside the brumble bush: complessità e riaffermazione delle scienze umane' (2006) 3 Riv crit dir priv 481-488; David J. Gerber, 'Method, Community & Comparative Law: An Encounter with Complexity Science' (2011) 16 Rog Will Un L Rev 114; Giuseppe Martinico, 'Asymmetry and Complex Adaptive (Legal) Systems: The Case of The European Union' (2014) 21 Maast J Eur Comp L 281.

[23] Philipp Hacker, 'Regulating under Uncertainty about Rationality: From Decision Theory to Machine Learning and Complexity Theory' in Stefan Grundmann, Philipp Hacker (eds.), *Theories of Choice. The Social Science and the Law of Decision Making* (Oxford University Press 2020). The programmer's main job is to define the characteristics and capabilities of the agents, the actions they can perform and the characteristics of the environment in which they are placed, as well as, possibly, the effects of their action on the environment itself.

[24] Friedrich August Hayek, 'The Theory of Complex Phenomena', in Friedrich August Hayek (ed.), *Studies in Philosophy, Politics and Economics* (Routledge & Kegan Paul

For what it concerns specifically the two crucial features of transparency and explainability, which are relevant for the goal of autonomy protection, technological tools enable human experts to improve the understanding of the connection between the system's inputs and outputs, intervening at the programming stage with the task to reduce the technology-based opacity from the very beginning, or through subsequent actions.[25]

Thus, complexity science is functional in understanding social dynamics. There is, for example, an analogy between artificial intelligence and legal systems: they are composed of several interconnected and dynamic units. This harks back to the concept of legal transplant that leads the researcher to consider which elements impact reality, also through other research methods.

The complexity of legal systems requires research tools and approaches suitable to overcoming epistemic barriers.

From this last perspective, the openness of comparison as a method can offer vital support to understanding the cognitive process based on categories which organize legal knowledge. Among other things, when such categories are based on cognitive errors, there is a risk that they turn into rigid cages to prevent the progress of knowledge.[26]

3.1 From vulnerabilities to digital vulnerability

Today, one of the concepts discussed mainly by scholars is vulnerability.[27] Indeed, choice architectures impact on consumer

1967). Some scientific phenomena are 'simple' and are predictable through quantitative methods. On the contrary, complex phenomena refer to systems whose elements do not interact linearly way and where the number of characteristics related to their interaction is too high to be understood by scientific observers. While nonlinear systems can be scientifically modeled, interactions are not quantitatively identifiable.

[25] Grochowski, Jablonawska, Lagiona, Sartor (n 184 Ch. II).

[26] On the role of classifications and taxonomies in organizing knowledge, see Giovanni Pascuzzi, 'Conoscere comparando: tra tassonomie ed errori cognitivi' (2017) 4 DPCE 1179 ss. See also Giovanni Pascuzzi, *La creatività del giurista. Tecniche e strategie dell'innovazione giuridica* (il Mulino 2018) 181, where the classification operation is analysed.

[27] A recognition and update, full of insights, of the debate was presented at the conference Digital Vulnerability in European Private Law (2nd Colloquium on the Law of the Digital Economy), held on 15 and 16 June 2023, at the University of Ferrara. However, the debate toward the need for a new concept of vulnerability in European contract law is not new; among others, see Mateusz Grochowski, 'Does European Contract Law Need a

autonomy, firstly, focusing on a new understanding of the benchmark based on which a commercial practice must be assessed,[28] which is composed by two basic concepts: the average consumer and the vulnerable consumer. The two concepts are interdependent on each other, and they can't be viewed separately, at least from a perspective of private law. Consumer law essentially tends to protect users as the weaker party in commercial relationships. It enables consumers to act as active and autonomous market players.[29] For practical reasons, the two notions will be explored separately (sections 3.1 and 3.2), to emphasize how their evolution marks a parallel trend towards the incidence of bias on the decisional process in the digital consumer meaning.

The current paragraph sketches out the evolution of the concept of vulnerability. In particular, the trajectories relate to: (i) the change from vulnerability, as a concept relating specific groups of persons to a general context-dependent feature where 'external' elements of the digital environment impact every digital consumer; (ii) the blurring of lines between different categories of law and different European policies due to the multidimensional and dynamic nature of digital vulnerability, which require further translation into manageable issues functional to providing a whole protection.[30]

Under the first point (i), it is worth moving from the current concept of vulnerability based on specific groups. Notably, the discipline is provided under European consumer law particularly by the UCPD.

Starting from the legislative definition, Article 5 (3) UCPD describes the vulnerable consumer as a member of a 'clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee'. A limited

New Concept of Vulnerability?' (2021) 4(10) Journal of European Consumer and Market Law.

[28] Lisa Waddington, 'Reflections on the Protection of 'Vulnerable' Consumers under EU Law' (2014) 2 Maastricht Faculty of Law Working Paper, available at <https://ssrn.com/abstract=2532904>.

[29] Natalie Helberger, Marijn Sax, Joanne Strycharz *et al.,* 'Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability' (2022) 45(2) J Consum Policy 178.

[30] Lastly, the OECD report of June 26 2023 introduced the topic by describing consumer vulnerability as a «complex and multi-dimensional concept that has no globally accepted definition». OECD (digital Economic Papers), 'Consumer vulnerability in Digital Age', June 23 n. 355 available at: <https://www.oecd-ilibrary.org/science-and-technology/consumer-vulnerability-in-the-digital-age_4d013cc5-en> accessed 29 June 2023.

role of the clause emerged during recent years in legal literature and case law.[31]

The provision must, first of all, be framed in the broader theoretical context of vulnerability, as arose over the years in EU law and case law, to understand that the constrains of the traditional category of vulnerability in circumstances where dark patterns damage consumer, is not a novel issue. Many other past situations underlined the inadequacy of the unique category of vulnerability in protecting many kinds of disadvantaged consumers.[32]

To sum up, the legislative vulnerable consumer referred to Art. 5(3) UCPD focuses on 'internal' consumer characteristics that affect their ability to adequately deal with commercial practices (mental or physical infirmity, age, or credulity). In cases where vulnerability was a factor for assessing whether a practice qualifies as either misleading or aggressive, literal interpretation leads judges to consider the perspective of a particular group of vulnerable consumers.

Enlarging the frame of references for vulnerability, with particular attention to situations where the consumer is acting under the pressure of advertising, advances in vulnerability literature have criticised the approach of identifying groups of vulnerable users because it appears disconnected from social reality.[33] Even the distinction between average and vulnerable consumer introduced by the UCPD has been considered too rigid due to the fact only members of one of the consumer's groups considered vulnerable (i.e., mental or physical infirmity, age or credulity) should be ensured of a higher level of protection.[34]

Distinguished scholars proposed a different interpretation of vulnerability, essentially opposite to the one expressed by the UCPD. This proposal pointed out that every consumer can be vulnerable depending on

[31] Helberger, Marijn Sax, Joanne Strycharz (n 29) 179.

[32] Lisa Waddington, 'Vulnerable and Confused: The Protection of "Vulnerable" Consumers under EU Law' (2013) 38 European law review 757-782.

[33] Joel Anderson, 'Autonomy and vulnerability entwined' in Catriona Mackenzie, Wendy Rogers, Susan Dodds (eds.), *Vulnerability: New Essays in Ethics and Feminist Philosophy* (Oxford University Press 2014) 134-161: «a person is vulnerable to the extent to which she is not in a position to prevent occurrences that would undermine what she takes to be important to her». Thus, vulnerability is about one's relation to the world, the forces (social, physical, technical) in the world that can affect anything one deems important, and one's (lack of) control or power over those forces.

[34] Geraint Howells, Christian Twigg-Flesner, Thomas Wilhelmsson, *Rethinking EU Consumer* (Taylor & Francis 2017).

the situation,[35] meaning that vulnerable consumers are not the exception: they are the rule because they all can be constantly manipulated.

In the BEUC report, this is referred to as digital asymmetry because, according to the study 'the distinction between external and internal digital vulnerability can be neatly translated into the UCPD through the concept of digital asymmetry'.[36]

Asymmetry entails businesses having a powerful position that cannot be balanced out simply by providing the consumer with information and evaluating whether the average consumer/vulnerable consumer understands it. Instead, digital vulnerability might entail another understanding of consumer vulnerability.

To understand vulnerabilities in the digital society, it is essential to realise the properties of such digital choice architectures. Digital choice architectures can be developed on a much larger scale with fewer chances for the consumer to detect them. This consists of behavioural manipulation, exploitation of vulnerabilities, omnipresent personalization affecting freedom of choice, and the rise of the largest digital platforms. Contemporary businesses do not limit themselves to targeting clear vulnerabilities; entirely on the contrary, the real competitive edge resides in identifying circumstances and personal characteristics that make a person vulnerable but have not yet resulted in actual vulnerabilities.

Digital choice architectures are designed to infer vulnerabilities, that can be considered the product of digital consumer markets. As consumers keep using the same services, apps, or platforms over time, the commercial entities offering those services, apps, or platforms will be able to collect and analyse more user data and, as a result, be better able to identify exploitable vulnerabilities. So far, the usual asymmetrical nature of commercial relationships become even more significant.

[35] Martha Albertson Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2008) 20(1) Yale Journal of Law & Feminism.

[36] The non-legal literature uses 'digital vulnerability' and 'vulnerability'. In European consumer law, vulnerability is a loaded term, like weakness. That is why this study proposes a different terminology that does justice to both dimensions of 'vulnerability', namely the external structural and the internal-dispositional. The notion of digital asymmetry avoids both traps, i.e. the vulnerability trap and the weakness trap. Regulatory attention should shift from defining vulnerability or sorting out particular users under the concept of vulnerability towards tackling the sources of vulnerability, which comprise digital asymmetry.

A similar critical consumer literature also expressed concerns about tracing a sharp distinction between vulnerable and average consumers.[37]

Following this path and switching to the second emphasised point (ii) of this paragraph, European policy documents demonstrate the transposition and dissemination of academic insights towards vulnerability, opting previously for abandoning the static definition.[38] The fact that some consumers may be more vulnerable than others determine a dynamic nature of the concept of vulnerability, which depends on 'external' factors: including contextual, relational, and situational factors.[39]

The issue was even more discussed with regards to the increasing of new forms of personalized strategies based on individual biases, weaknesses, preferences, and needs that can make every consumer vulnerable.[40]

Algorithms and digital design can catch the circumstances under which persons can be rendered vulnerable with important implications for consumer law (e.g. market environment). According to Helberger:

[37] In general, the consumer research literature relates to two main streams of thought: vulnerability due to disadvantages and marketer manipulation. Stacey M. Baker, James W. Gentry, Terri Rittenburg, 'Building Understanding of the Domain of Consumer Vulnerability' (2005) 25(2) Journal of Macromarketing 128-139. This more universal understanding of consumer vulnerability probably goes too far for some. Reich, for example, suggests that the concept of consumer vulnerability needs to be distinguished from the concept of consumer weakness to avoid expanding the concept too far (Reich, 2016, 141). Norbert Reich, 'Vulnerable consumers in EU law', in Dorota Leczykiewicz, Stephen Weatherill (eds.), *The Image of the Consumer in EU Law: Legislation, Free Movement and Competition Law* (Bloomsbury Publishing 2016) 141.

[38] London Economics, VVA Consulting, & Ipsos Mori consortium (2016). Consumer vulnerability across key markets in the European Union. Study for the European Commission, DG Justice and Consumers, Brussels. <https://ec.europa.eu/ info/ sites/ info/files/ consumers- approved- report_en.Pdf>; European Commission (2016). Understanding consumer vulnerability in the EU's key markets. Factsheet, Brussels. <https://ec.europa.eu/info/sites/info/files/consumer-vulnerability- facts heet_en.pdf.> accessed 1 June 2022.

[39] European Commission, 2016 In a more recent communication, the European Commission (2016) defined the vulnerable consumer as: «a consumer, who, as a result of socio-demographic characteristics, behavioural characteristics, personal situation, or market environment: Is at higher risk of experiencing negative outcomes in the market; Has limited ability to maximise their well-being; it has difficulty in obtaining or assimilating information; it is less able to buy, choose or access suitable products; or it is more susceptible to certain marketing practices». European Commission (2016). Understanding consumer vulnerability in the EU's key markets, Factsheet, Brussels.

[40] Ryan Calo, 'Digital Market Manipulation' (2013) 82 Geo Wash L Rev 995, 1033.

‘with digital practices, commercial messages are only one part in a larger, systemic approach to influencing consumer behaviour. The message is part of the system and can no longer be separated from the technical infrastructure that generates it, because it is a result of […] an ‘adaptive persuasive system’. Accordingly, to evaluate commercial practices in terms of their fairness, it is not enough to evaluate the message; the systemic set-up and the way technology shapes the relationship between consumer and advertiser should also figure prominently in such an analysis’.

Contemporary digital choice architectures offer an infrastructure to identify and exploit a wide range of vulnerabilities by design. An additional perspective that requires elaboration is the relational nature of vulnerabilities in the digital society. People are not (just) vulnerable in total isolation; more often than not, it is precisely people’s relational ties to others that cause them to be influenced.

The needed change for the notion in question also induces rethinking the applicable legal framework because, while technology and human biases impact the effectiveness and appropriateness of the information and consent paradigm, how the information is presented has also acquired great importance.

In sum, the UCPD will only become a powerful instrument if the hypothesis that external-structural asymmetries would be qualified as aggressive practices in line with Articles 8 and 9 UCPD or if its basis is rethought: indeed, the clause on misleading practices focuses on the ‘information component’ of commercial practices, but the more significant and more important question pertains to the structural power relations that are introduced by contemporary digital choice architectures.

When considering digital asymmetry, lawyers should make space for interpretation beyond power imbalances, getting away from the individual responsibilities of the ‘stronger party’ and remarking on the structural effects of how the technology is used.

Digital asymmetry must not be reduced to information asymmetry; even suitable legal protection does have to be reduced to information infringement: the consumer is structurally and universally unable to understand the digital architecture, and information in whatever form cannot remedy the existing asymmetry.

The consequence is that a solution in the existing body of consumer law must tackle the structural side, the digital architecture, by means other than information. Thinking digital architecture involves legal experts from the very beginning of the design process: this could contribute to preemptively investigating the issue of coordination between applicable regulations, as well as managing the integration between law and behavioural sciences knowledge about consumer's attitudes and behaviour. Since the beginning, this approach could also help tackle digital asymmetry, as a structural unavoidable condition, reducing inequality.

There are different opinions about how to frame and discipline digital asymmetry. Some consider the interpretation of digital asymmetry in the form of data exploitation strategies under the prohibition of misleading actions and misleading omissions as a dead-end street.

Others start from the premise that data exploitation strategies could and should be regarded as commercial practices and that the scope of application of the UCPD remains open, above and beyond the GDPR. A holistic perspective requires including data exploitation policies in the analysis, which are enshrined in standard terms and can, therefore, be submitted to judicial control under the UCTD. The three legislative measures, though different in scope, are claimed to be based on a common denominator: ensuring that consumers are treated fairly when acting as data subjects as regards their privacy concerns, as addressees of commercial practices, or as contracting partners.

In this manner, the EU is institutionalizing market fairness, only if a common benchmark cuts across the different legislative elements. The legislative architecture of the fairness test has to result from the interplay between standardized forms of data exploitation strategies and non-standardized policies, with which different forms of legal remedies can be associated.

As carefully suggested in Chapter II, it is possible to discover elements inherent to the current provisions that not only define the scope but also lay the ground for the control architecture.

For instance, Article 2 (1) of the GDPR applies to the processing of personal data wholly or partly by automated means.

Then, several provisions of the UCPD show the analogous footholds: Article 2 (1) pointed out that commercial practice means any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers; Article 11a (1) indicates that consumers harmed by unfair commercial practices shall have access to proportionate and effective remedies, including compensation for damage suffered by the consumer and, where relevant, a price reduction or the termination of the contract. Member States may determine the conditions for the application and effects of those remedies, and they can take into account, where appropriate, the nature of the unfair commercial practice, the damage suffered by the consumer and other relevant circumstances. Based on Article 3 (1), a contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer. Point (2) of the same article indicates that a term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has, therefore, not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract.

Moreover, even when referring to vulnerability, attention should be drawn to the legislative architecture of the fairness test. It is important to connect this concept to the interplay between standardized forms of data exploitation strategies and non-standardized policies and the associated forms of legal remedies.

To conclude, in the EU agenda, vulnerability seems to go beyond consumer law, to consider, for example, to what extent abuse of the digital market will impact on collective and individual rights, and generally following the path of researching an intersectoral legal regulation and remedy area.

3.2 From the 'average consumer' prototype to the digital vulnerable consumer

Because of the changes implicated by the renovated idea of vulnerability, better defined now as digital vulnerability, the concept of the average consumer has undergone an equivalent transformation. The notion of consumer represents a centrepiece of European consumer protection law and has served as a benchmark for legislation and law enforcement. Indeed, the whole idea of dark patterns sits uneasily with the UCPD benchmark of an average consumer, as it has traditionally been understood.

The 'average consumer' paradigm was first introduced by the ECJ, then crystalized in European private legislation, leaving very little room for exceptions. Initially, only the exception of the vulnerable consumer was introduced by Art. 5 of the Directive 2005/29/EC (UCPD). Subsequently, it was also referred to the Consumer Rights Directives (recital 34 of the CRD). Rooted in recital 18 and Art. 5(2) UCPD, the benchmark of the average consumer is reasonably well-informed, observant and circumspect, considering social, cultural and linguistic factors. In its extensive case law, the ECJ tends to refer to the 'weak' consumer who requires protection.[41]

The concept of 'vulnerable consumer groups' was already part of Directive 97/55/EC, which amended Directive 84/450/ECC concerning misleading advertising, including comparative advertising where, however, the notion was only referred to in recital 22 and employed to enable a Member State to maintain, or introduce, stricter bans on marketing methods or advertising which target vulnerable consumer groups. The Directive is now repealed by Directive 2006/114/EC, which applies only to business-to-business relationships, and the reference to the vulnerable consumer has accordingly been removed.

The original scope of the provision was to prevent the exploitation of consumers whose characteristics make them particularly vulnerable to unfair commercial practices, such as children or people with specific disabilities. In practice, a fairness test must be balanced differently in case of individual fragilities (physical disease, psychological suffering, socioeconomic problems, such as poverty, age (minors and elderly people), allowing the modification of the criteria in the context of the proportionality test.

This is the authentic legal meaning of average consumer and vulnerability, but the concepts are wide and described many ways by legal literature over the years.

From a *de jure condito* perspective, this average consumer is still relevant when assessing the fairness of a particular practice.

This concept has been criticized for being a prototypical personification of an average consumer: ideally, a UCPD average consumer does not have cognitive biases, which is, of course, unrealistic. Based on behavioural studies, all people, or at least the (average) majority, even educated people, experienced cognitive biases. Empirical studies demonstrate some dark patterns greater or lesser effectiveness within heterogeneous population samples.

Nevertheless, the emergence of the dark pattern phenomenon does not represent the first occasion for lawyers to express such reservations.[42] Case

[41] Hans-W. Micklitz, Norbert Reich, *European Consumer Law* (Intersentia 2014) 771-808.

[42] For several years, many academic scholars have underlined the limits of the notion. Among many, see, in particular, Cristina Poncibò, Rossella Incardona, 'The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution' (2007) 30 (1) Journal of Consumer Policy Issue 21-38. Authors underlined that an overly simplistic concept with little correspondence with the real world of individual consumer

law, too, over the years, has considered the evolution from *homo oeconomicus* to *homo heuristicus* prototypes.[43]

Earlier famous ECJ cases, such as *Mars* ruling,[44] testified to the adoption of the traditional consumer standard as such.

Instead, more recent case law, assuming the flexibility of the standard, orientates the content to the contributions of behavioural economics and cognitive science. Teekanne case, on a package design of foodstuffs, is a well-recognized case for stating the necessity to 'update' to the concept.[45] It has also been interpreted by scholars by the findings of behavioural economics.[46] The Court ruled that it is unlawful to use a package design for a fruit tea that gives the impression that an ingredient is present when it is not in fact, and this is apparent solely from the list of ingredients on the fruit tea's packaging. The listing of ingredients in compliance with food labelling requirements may, even though correct and comprehensive, be incapable of sufficiently correcting a consumer's erroneous impression from the overall package design.

behaviour should be reinterpreted more flexibly or even abandoned to mirror consumer behaviour more effectively. See also: Lisa Waddington, 'Vulnerable and Confused: The Protection of "Vulnerable" Consumers under EU Law' (2013) 38 European law review 757-782.

[43] Edoardo Bacciardi, 'Lo standard del consumatore medio tra *homo oeconomicus* e *homo heuristicus*' (2023) 1 Accademia 77-99.

[44] Case C-470/93 *Verein gegen Unwesen in Handel und Gewerbe Köln eV* EU:C:1995:224 [1995] See also C-220/98 *Estée Lauder Cosmetics GmbH & Co. ORG v Lancaster Group GmbH*, EU:C:1999:425 [1999]. The origins of ECJ case-law based on the average consumer can be traced in Gut Springenheide (see Ch I).

[45] Case C-195/14 *Teekanne* EU:C:2015:361 [2015]. Different authors emphasised the need to reviewing the jurisprudential notion of consumer, see: Kai Purnhagen, 'More Reality in the CJEU's Interpretation of the Average Consumer Benchmark – Also More Behavioural Science in Unfair Commercial Practices?' (2017) 8(2) European Journal of Risk Regulation 437-440. See more in Chapter III.

[46] Hanna Schebesta, Kai Purnhagen, 'The Behaviour of the Average Consumer: A Little Less Normativity and a Little More Reality in CJEU's Case Law? Reflections on Teekanne' (2016) European Law Review 595. There is some discussion in the literature as to what extent this list is exhaustive or not: Bram Duivenvoorde, 'The protection of vulnerable consumers under the unfair commercial practices directive' (2013) 2(2) Journal of European Consumer and Market Law 69-79; Geraint Howells, Christian Twigg-Flesner, Thomas Wilhelmsson, *Rethinking EU consumer law* (Routledge 2018). Maurits Kaptein, Panos Markopoulos, Boris de Ruyter, Emile Aarts, 'Personalizing persuasive technologies: Explicit and implicit personalization using persuasion profiles' (2015) 77 International Journal of Human-Computer Studies 38-51; Hans – G. Micklitz, Monika Namyslowska, Müchener Kommentar Zum Lauterkeitsrecht (2020), Art. 8 22.

Therefore, if the concept is qualified as a flexible standard, it should also be able to change as more behavioural insights are gained and underlined by academics commenting on case law.[47]

One could counter that the concept of 'average' is an indicator of the perception that not everyone is alike. However, the problem then might be that the difference is measured only through an evaluation of three pre-defined, similar and somewhat unrealistic elements (well-informed, observant, circumspect).

Even though the concept has been rightly criticized, the challenge is that we undoubtedly require benchmarks for businesses when they develop advertising, consent forms and other types of information or structures, as well as when they shape the digital architectures of their websites. A benchmark supports collective actions and removes the focus placed upon the individual consumer, and their consent/understanding.

Recently, the request for preliminary reference judgement was submitted by the Italian Consiglio di Stato to the ECJ (Consiglio di Stato, sez. VI, 10.10.2022, n. 8650):[48] it concerns the interpretation of the notion of 'average consumer', in light of behavioural law and economics insights. In practice, the highest Italian administrative jurisdiction asks (*sub* let. a) whether the concept of 'average consumer' canonized by the Directive 2005/29/EC fits squarely within the «classic concept of *homo economicus*», or if the archetype of the consumer should instead be redefined, considering the 'findings of the most recent theories on bounded rationality'.[49]

[47] Kai Purnhagen, 'More Reality in the CJEU's Interpretation of the Average Consumer Benchmark – Also More Behavioural Science in Unfair Commercial Practices?' (2017) 8 European Journal of Risk Regulation 437, 439.

[48] Consiglio di Stato italiano (Sez. VI), 10 October 2022 No. 8650 <https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza?nodeRef=&schema=cds&nrg=202110361&nomeFile=202208650_18.html&subDir=Provvedimenti> accessed 3 January 2023.

[49] The above mentioned ruling also concerned: (b) whether a commercial practice, due to the framing of the information (framing) is functional to give a choice which can appear to be mandatory and without alternatives, taking into account Article 6, paragraph 1, of the Directive, which considers misleading a commercial practice that in any way deceives, or can deceive, the average consumer «even in its overall presentation»; (c) whether the Unfair Commercial Practices Directive justifies the power of the National Competition and Market Authority (once the danger of psychological conditioning linked to: 1) the need in which those seeking financing normally find themselves, 2) the complexity of the contracts submitted for signature by the consumer, 3) the contextuality of the offer submitted in conjunction, 4) the short time allowed for the subscription of the offer), to provide for a derogation from the principle of the possibility of combining the sale of insurance products with the sale of unconnected financial products by imposing a period of 7 days between the signatures of the two contracts; (d) if, in relation to this repressive

Ultimately, the expected ECJ interpretative judgment, considering the interplay between law, behavioural science, and consumer behaviour, will have to decide whether to abandon the traditional notion of the average consumer because it is unrealistic or to update concerning 'external' factors, more in line with real consumer behaviour. Given the relevance of cognitive aspects and the specificities of digital architectures, a possible shift could be from average consumer to vulnerable consumer.

Alongside ECJ case law, the political and academic debate addresses the same topic from the same perspective. With the response to question No. 19 of the ELI report, dedicated to 'Adapting the Concept of the 'Average Consumer' or 'Vulnerable Consumer',[50] the Institution aims to find out if the concept of the 'average consumer' or 'vulnerable consumer' could be adapted, or complemented by additional benchmarks, or factors. The report's authors recognized that the standard's flexibility encompasses all situations at all times, and it can change with the development of society.[51] They also underlined that such flexible standard does not guarantee legal certainty. Consequently, businesses could not know the expected standard

power of aggressive commercial practices, the Directive (EU) 2016/97, and in particular Art. 24 paragraph 3 thereof, which precludes the adoption of a measure by the Competition and Market Authority adopted on the basis of Art. 2, d) and j), 4, 8 and 9 of Directive 2005/29/EC and the national transposing legislation adopted after the rejection of an application for commitments following the rejection of an investment services company, in the case of combined sale of a financial product, and an insurance product not related to the first – and in the presence of a danger of conditioning of the consumer linked to the circumstances of the concrete case inferable also from the complexity of the documentation to be examined – to grant to the consumer a *spatium deliberandi* of 7 days between the formulation of the combined proposal and the signing of the insurance contract; (e) If the aggressive practice considered the mere combination of two financial and insurance products could end up in an act of regulation not allowed and would not end up placing the burden on the professional (and not on the AGCM, as it should be) (difficult to absolve) to prove that this is not an aggressive practice in violation of Directive 2005/29/EC (especially as the abovementioned Directive does not allow Member States to adopt more restrictive measures than those defined by it , even in order to ensure a higher level of consumer protection) or, on the other hand, if such a reversal of the burden of proof does not exist, provided that, on the basis of objective evidence, the real danger of conditioning the consumer in need of financing a complex matched offer is considered.

[50] ibid

[51] Legal traditions differ in the Member States, where the approach to a large part of private law has traditionally been based on principles and broad standards reflecting a pragmatic approach to resolving disputes, standards like 'average/vulnerable consumer' might not seem so problematic if the standards are applied in accordance with developments in society. The uncertainty, however, is still there.

of such a consumer in advance, with obvious criticalities for providing adequate information.

Therefore, one can argue that the 'average consumer' of the UCPD is at risk of being manipulated by dark patterns and that the same concept must be interpreted in such a way that it incorporates biases.

Indeed, according to one of the conclusions of the BEUC study: the average consumer's ability to discern the use of dark commercial practices in the digital environment is limited.

Findings demonstrated that there is a significant portion of average consumers make inconsistent choices, which may suggest that in the online context, both average and vulnerable consumers are susceptible to unfair practices. This is why even when consumers are well informed and given enough time to make a transactional decision, their choices are often still inconsistent with their preferences.[52]

Other recent empirical studies confirm that 'the level of awareness did not play a significant role in predicting their ability to resist manipulative designs. This finding implies that raising awareness on the issue is not sufficient to shield users from the influence of dark patterns'.[53]

In conclusion, there is no guarantee that the ECJ will engage with behavioural studies, to profoundly reviewing the standard notion. Therefore, it should be clarified that the 'average consumer' has biases that can be exploited using dark patterns. This is also why, in line with the conclusions of recent public academic events,[54] it could be argued that observations about the potential substitution of the average standard with the standard of the 'vulnerable consumer', or the 'average digital consumer' could be more realistic, without forgetting the necessity of avoiding the risks of a generalization of behaviourism.[55]

4. Towards the suitable legal model

To tackle the problem of the necessary multidimensional protection of the fundamental right to autonomy, even narrowing down the analysis to

[52] Lupiáñez-Villanueva, Boluda, Bogliacino, Lechardoy, Rodríguez de las Heras Ballell, (n 20 Ch. II), 120.

[53] ibid 8.

[54] E.g.: The 2nd Colloquium on the Law of the Digital Economy on 'Digital Vulnerability in European Private Law', organized by Ferrara University, 15-16 June 2023.

[55] Bacciardi (n 43) 86.

the private law perspective of consumer autonomy requires reflecting on suitable business and regulatory models able to capture the complexity of empirical situations within an evolving benchmark standard.

Nevertheless, the various forms of structural asymmetry (digitally mediated relationship, choice architecture, architectural infrastructure), the nature of the fundamental right under examination, and the different forms of power (e.g. economic and intellectual power) in the hands of businesses are all factors to take into account because of their impact on the balance between regulation (*ex ante* approach) and civil liability regimes (*ex post* approach). In other words, it should be considered to what extent it is necessary to go beyond the coordinated approach of the institutional complementarities (regulation and liability regimes) to enforce alternative regulatory instruments to address the specific challenges posed by digital architectures.[56]

Considering the applicable traditional legal approaches separately, the previous chapter offered many reflections to support them with a more relevant thinking towards the by design regulation.

To sum up the findings achievable from Chapter II. From an ex post perspective, and given its structural architecture, remedies available in case of misleading information are various: the hypothesis to qualify data exploitation strategies as commercial practices have far-reaching implications for exercising control parameters.

Data exploitation strategies should be understood as sales promotion measures, and it is an external element for the consumer, often becoming a source of digital vulnerability. Consequently, remedies cannot be based on actions for the breach of the information paradigm, which governs the assessment of misleading advertising. Remedies available must be found in many policies. While the GDPR provides some guidance on the formulation of privacy notices, it leaves room for interpretation because the notices published on different websites, vary widely in terms of the user interface, their functionality, content, and formulation. Nevertheless, a certain number of doubts exist when considering if GDPR provisions (e.g recital 43; Art. 7(4) are a suitable legal ground for ensuring the quality of the consent that does not exclusively depend on the data controller's

[56] On the evolutionary regulatory lines of the data-driven technologies it is relevant the following essay: Erica Palmerini, 'Algoritimi e decisioni automatizzate. Tutele esistenti e line evolutive della regolazione', in Luis Efrén Rios Vega, Lucia Scaffardi, Irene Spigno (eds.), *I diritti fondamentali nell'era della* digital mass surveillance (Editoriale Scientifica 2021) 209-244. See section 11, 233.

market power level. For example, a distinction based on firms' market power is not yet available and could help in this sense.

To consider a more general observation, if data exploitation is qualified as an unfair commercial practice, UCPD and consumer law will be applied; if data is collected and processed by an organization to extract economic value by exploiting its economic power, it will be identified as an anti-competitive practice, and remedies from competition law will be applied.

The problem with the multitude of remedies offered by the several involved policies is enforcement, also relating to ensuring that data used to develop Big Data and AI applications meet quality standards.

With regards to the *ex ante* perspective, looking at the pervasive role played by the GDPR, an accurate analysis deserves its 'one-size-fits-all law' model in the wake of a variety of technologies.[57] Practically, EU legislation in digital matters exerts direct and indirect influences on public and private actors around the world.[58]

Data-driven technologies introduce new risks and concerns for protecting consumer autonomy, which is not explicitly taken into account by EU data protection law. This means the current model is inadequate to provide the same protection and tools for many kinds of disadvantaged consumers who can fall under the general category of harms, or vulnerability. Instead, targeted measures based on the recognition of the diversity of all consumers would provide greater protection.

This profile also offers the occasion to reflect on the adequacy of the standard: GDPR addresses the processing of personal data by automated means.[59] Automation implies standardization, but it is also true that data may

[57] However, these requirements still need to change the overall regulatory structure. The GDPR does not use the language and concepts established in EU economic law, such as supplier, customer, and consumer, despite the overall objective of the GDPR to establish a regulatory framework for 'the free flow of personal data in the Internal Market', according to Article 1 (3) GDPR. There is a mismatch between the regulatory philosophy, the language, and the concepts, which insinuates a kind of neutrality on the part of the GDPR and the foundational role and function the GDPR plays for the governance of economic transactions.

[58] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020) 131; and Mariavittoria Catanzariti, Deidre Curtain, 'Data at the Boundaries of (European) Law: a first cut' in Deidre Curtin, Mariavittoria Catanzariti (eds.), *Data at the Boundaries of European Law* (Oxford University Press 2023) 1.

[59] Unlike the UCPD and the UCTD, the GDPR is not built around what is forbidden and what kind of marketing strategies are to be avoided. Quite to the contrary: the philosophy behind the GDPR is to lay down the requirements that the 'processor' (Article 4 (8) has to respect, i.e. the rules data controller should respect to comply with the law.

be used to target consumer groups or consumers individually. This means that the degree of personalization varies according to the algorithm used to evaluate the collected data.

In various passages of the previous chapter, the idea of reinforcing the regulation *by design* emerged as an ideal approach which deserves further attention because it looks suitable to implement the ex ante regulatory framework through interdisciplinary collaboration.

For all these reasons, it is worth exploring the role and potentiality of legal design (section 4.1.), focusing on the legal model for legislating and the prerequisite to set it, such as interdisciplinary research method (section 4.3).

4.1 The legal design

In current times, the effort to combine regulatory intents with attention to their legal design has received much attention from scholars and policymakers.[60] Indeed, by designing choice mechanisms aware of data subject informational vulnerabilities, the data controller will be able to support the consumer's autonomy and empower him or her.

Legal design patterns are essential problem-solving tools that can prevent disputes and be reused for coping with recurring problems,[61] triggering, for example, a more transparent and understandable communication,[62] based on recognized good practices and efficient standards.

This does not mean that the GDPR does not define thresholds for collecting and recording data.

[60] Margaret Hagan, 'Law by Design' (2016), online at <https://lawbydesign.co/>; Dan Jackson, Jules R Sievert, Miso Kim, Sankalp Bhatnagar 'What legal design could be: Towards an expanded practice of inquiry, critique, and action' in Dan Lockton, Sara Lenzi, Paul Hekkert, Arlene Oak, Juan Sádaba, Peter Lloyd (eds) DRS2022: Bilbao (Design Research Society 2022) <https://doi.org/10.21606/drs.2022.281> accessed 26 June 2023; Barbara Pasa, Gianni Sinni, 'New Frontiers of Legal Knowledge: how design provotypes can contribute to legal change', in Rossana Ducato, Alain Strowel (eds), *Design(s) for Law* (Ledizioni 2023, forthcoming). For an extensive reading, see: Rossana Ducato, Alain Strowel (eds), *Legal Design Perspectives Theoretical and practical insights from the field* (Ledizioni 2021).

[61] Cristopher Alexander *et al.*, *A Pattern Language – Towns, Buildings, Construction* (Oxford University Press 1977).

[62] Arianna Rossi, Rossana Ducato, Helena Haapio, Stefania Passera, 'When Design Met Law: Design Patterns for Information Transparency' (2019) 122123(5) Droit de la consommation 71, part. 87. The Authors describe the emerging discipline of Legal Design to contribute to and collect existing legal information design patterns meant to implement the principle of transparency in consumer and data protection law. Authors presented

Initially, design patterns were practical techniques mainly employed in computer science and other fields.[63] Only belatedly, they were employed for digital architectures, gaining a crucial role in legal design.[64] Legal design can be identified as a discipline that combines law, technology, and design to create user-friendly legal documents and, more generally, make the legal system more accessible to people.[65]

Thinking from the perspective of legal design means focusing on ex ante regulation, adopting what the Nordic School identifies as a Proactive Law approach: this is a new dimension added to Preventive Law,[66] based on which it has been commonly said that thinking like a lawyer is not sufficient.[67] Thus, legal design is based on proactive law approach, which is 'about enabling and empowering – it is done by, with and for the users of the law, individuals and businesses; the vision here is of a society where people and businesses are aware of their rights and responsibilities, can

operative tools that demonstrate how the legal principle of transparency can be translated into practice through behavioural and design lenses.

[63] Erich Gamma *et al.*, *Design Patterns: Elements of Reusable Object-Oriented Software* (Pearson Education India 1995).

[64] Over the last few years, several legal design patterns and pattern libraries have emerged from practice. Arianna Rossi, Monica Palmirani, 'Legal Design Patterns: Towards A New Language for Legal Information Design', in Erich Schweighofer, Franz Kummer, Ahti Saarenpää (eds), *Internet of Things. Proceedings of the 22nd International Legal Informatics Symposium IRIS 2019* (Editions Weblaw 2019) 517-526.

[65] The concept of legal design draws on design thinking, a methodology to solve problems in a creative and human-centric way. See, for instance, Roger L Martin, *Design of Business: Why Design Thinking is the Next Competitive Advantage* (Harvard Business School Press, 2009); Chiara Rauccio, 'How legal design can improve data protection communication and make privacy policy more attractive' (2021) 1 European Journal of Privacy Law & Technologies.

[66] On the emerging proactive law see the Nordic School of Proactive Law, available at <http://www.juridicum.su.se/proactivelaw/main>. See, in general, on the topic: Helena Haapio, 'Introduction to Proactive Law: A Business Lawyer's View', in Peter Wahlgren (ed.), *A Proactive Approach, Scandinavian Studies in Law* (2006) 49, Stockholm, Stockholm Institute for Scandinavian Law 21-34.

[67] For these Authors, it is important to think about what users are trying to reach and then present information in a way that can be readily put into action by the users to achieve their goals. To make this happen, to promote 'legal well-being', and to prevent cognitive accidents, it is crucial to think like designers. Sless affirmed: «we came to realize that organizations often ask the wrong question. They ask: 'What information should go into the document?,' when they should be asking, 'What actions should people be able to perform, easily and quickly, with the information given?» David Sless, 'Designing Documents for People to Use' (2018) 4(2) The Journal of Design, Economics, and Innovation 125-42, 131.

take advantage of the benefits that the law can confer, know their legal duties to avoid problems where possible, and can resolve unavoidable disputes early using the most appropriate methods'.[68]

With these words, recital 1.5 of the Opinion of the European Economic and Social Committee on 'the proactive law approach: a further step towards better regulation at EU level',[69] describes that the future-oriented approach aims to promote what is desirable and maximizes opportunities while reducing risks.

With the scope to choose regulatory tools, it is important to measure how the goals are achievable for EU citizens and businesses because predictability, sustainability and foreseeability are basic requirements for a well-functioning, citizen- and business-friendly legal environment.

To act in advance by including effective rules by design allows meaningful and direct communication to the recipients of the rules.

The primary intent is to control a situation and nudge the determinant factors instead of applying remedies once damage arises.

This goal will encounter the European purpose to set up a so-called Better Regulation,[70] by providing a new way of thinking, taking as a starting point the real-life needs and aspirations of individuals and businesses.[71]

Consequently, the strengths of the preventive legal approach, which pragmatically is concretised by an optimal mix of regulatory means, will imply an active and effective participation of private powers, as well as the consideration from the very beginning of not only economic and legal but also social and ethical aspects, constructing consumers-oriented solutions.[72] This aim implies the need to share a standard understanding of terms, definitions, descriptions, limitations and interpretations within common frames of reference, focusing on the model laws approach, rather than on detailed harmonisation.

[68] Opinion of the European Economic and Social Committee on 'The proactive law approach: a further step towards better regulation at EU level'.

[69] European Economic and Social Committee, Opinion of the on 'The proactive law approach: a further step towards better regulation at EU level', OJ C 175/27 Official Journal of European Union 28 July 2009.

[70] On the objectives of the Better Regulation Agenda see <https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation_en> accessed 22 April 2023.

[71] Recommendation 2.3 of the Opinion (ibid).

[72] Empathy is at the basis of design thinking: see Gerlinde Berger-Walliser, Thomas D. Barton, Helena Haapio, 'From Visualization to Legal Design: A Collaborative and Creative Process' (2016) 54(2) American Business Law Journal, Summer 347-392, California Western School of Law Research Paper No. 16-11.

The methodology for obtaining this result would start from collaborative actions between several stakeholders.[73] Projects should be required to be based on an interdisciplinary approach apt to involve lawyers, ethicists, communication experts, informatics. The essential importance of interdisciplinarity deserves further attention to grasp how to work in this direction; this is why a specific consideration will be dedicated within paragraph 4.3.

From a more practical point of view, the necessary research tools are exploratory techniques, like 'sketching' or 'mapping' out different solutions, or even creating the so-called 'provotypes'. They are all ways to test different solutions or potential scenarios.[74]

The increasing interest in such perspectives testifies to the changing nature and origins of the contemporary process of legal change, which predominantly depends on the informal processes, criptotypes, and social practices[75]. Nowadays, legal change is complex and non-linear, often provoked by the undistinguished action of domestic, national, transnational and global processes, as the interaction of a two-dimensional action, collective and individual.[76]

The implementation of different rules and principles by design, all functional to guarantee consumer autonomy, will capture all the instances for a renovated and more coordinated approach to autonomy when challenged by deceptive digital architectures.[77]

The reasoning toward the paradigms of transparency and fairness in the previous chapter has already demonstrated the necessary change of the protection model in order to avoid deception by digital architectures.[78]

[73] ibid

[74] These are solution-based strategies typically used by designers, which not only help the expert to solve the problem better, but also help clients better understand the solutions offered to them: Gerlinde Berger-Walliser, Thomas D. Barton, Helena Haapio, 'From Visualization to Legal Design: A Collaborative and Creative Process' (2016) 54(2) American Business Law Journal, 347-392, California Western School of Law Research Paper No. 16-11.

[75] Pasa, Sinni (n 61).

[76] See Michele Graziadei, 'What does globalisation mean for the comparative study of law?' (2021) 16 Journal of Comparative Law 511.

[77] Amanda Perry-Kessaris, 'Legal design for practice, activism, policy and research' (2019) 46(2) Journal of Law and Society 185-210.

[78] Deirdre K. Mulligan, Kenneth A. Bamberger, 'Saving Governance-by-Design' (May 7, 2018) 106(3) California Law Review 697 <https://www.jstor.org/stable/26577731> accessed 23 June 2023.

Designers will play a pivotal, relevant role in constructing fairness. As scholars already noted, it is likely that as it happens in data protection law with the provision 26 GDPR, which imposes obligations onto app designers, new regulation about dark patterns in consumer law should impose consumer protection duties onto the designer community.[79]

'Fairness by design' setting involves designers. Such an extension to system design may not be relevant to the UCPD's objectives, but it would be essential for effective regulation to contrast dark patterns. To reach this aim, self-regulation tools, such as a specific code of conduct for designers could also be functional in setting up a higher standard than that provided by the UCPD. Supplements should be encouraged to end the current uncertainty and incompleteness found in the application of the UCPD to dark patterns.

Enhancement of industrial self-regulation might emerge with attention to the legal design. Corporate Digital Responsibility initiatives around the globe also guide the ethical use of digital technology and recommend measures that may help businesses be transparent and respect the consumer's freedom of choice. These modern exigencies expressed through soft law can be easier and more effectively considered if implemented by design.

Examples are already in place. The French data protection authority (CNIL) has developed cases-studies of user interfaces aimed at helping designers comply with the GDPR.[80] Similarly, the EDPB Guidelines 3/2022 provide practical recommendations and best practices for designers and users of social media platforms on assessing and avoiding dark patterns in digital platforms that infringe GDRP requirements.[81]

The objects that this design could focus on are various. Fairness by design and transparency have already been considered (Ch. II). The legal design can also include the principles and aims of competition law. Competition enforcers could then provide practical guidance on how firms could go about 'designing in' competition compliance. Thus, for instance, a useful principle derived from the related concept of privacy by design could be that firms should endorse the value of making proactive ex ante risk assessments and reducing the probability that algorithms will negatively affect competition.

[79] Ducato, Strowel (eds), (n 60).

[80] See <https://design.cnil.fr/> accessed 8 May 2023.

[81] See <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en> accessed 20 April 2023.

Beyond the implementation of specific goals and principles by design, the important role acquired by 'governance-by-design', meaning the general purposeful effort to use technology to embed values, could demonstrate that private powers could contribute to implementing the same democratic process of the legislative public powers.[82]

It is necessary to develop proper rules to guarantee effective public participation, purposeful debate, and relevant expertise to rely on governance by-design. 'Designing technology to 'bake in' values offer a seductively elegant and effective means of control' that requires maintaining a flexible design, privileging a human-centric approach, ensuring technical expertise and regulators' authority, and guaranteeing an open process of policymaking.[83]

Mainly, a user-centred approach, driving human forces behind the design process are humans is essential when regulating technologies.[84]

4.2 How to design fair algorithms? An open debate between lawyers and computer scientists

To do a step forward in constructing the protection of autonomy through digital architectures, it is necessary to consider the lively debate on the meaning of fairness in the context of decisions based on statistical predictions and machine learning models. Indeed, the issue of algorithmic fairness is a crucial topic of debate which involves mainly – but not exclusively – lawyers and computer scientists.[85] Barocas and Hardt emphasized that:

[82] There are opposite opinions. For example, Bamberger (n 78) underlined the risks governance by design can subvert public governance.

[83] Scholars pointed out rules to focus on the process of building out institutional capacity for rigorous and inclusive governance around the role of technology as a regulator (n 60).

[84] Tim Brown, 'Design Thinking' (2008) 84 Harv Bus Rev 86. See Torsten J. Gerpott, 'Dark Patterns in Web User Interfaces: Toward an Incentive-Based Policy Approach Supplementing Legal Provisions' (2022) 102(9) Wirtschaftsdienst 688-693; Batya Friedman, Peyina Lin, Jessika K. Miller, 'Informed consent by design', Security and Usability (2001) 503-530.

[85] Shira Mitchell, Eric Potash, Solon Barocas, Solon, Alexander D'Amour, Kristian Lum, 'Algorithmic Fairness: Choices, Assumptions, and Definitions' (2021) Annual Review of Statistics and Its Application. Corbett-Davies S, Pierson E, Feller A, Goel S, Huq A (2017), Algorithmic decision making and the cost of fairness, in Proceedings of the 23rd ACM SIGKDD international conference on knowledge discovery and data mining 797-806; Stefan Feuerriegel, Mateusz Dolata, Gerarhad Schwabe, 'Fair AI – challenges and

'entire disciplines have embraced mathematical models of optimal decision making in their theoretical foundations. Much of economic theory takes optimal decisions as an assumption and an ideal of human behaviour. In turn, other disciplines label deviations from mathematical optimality as 'bias' that invites elimination'.[86]

However, it is necessary to comprehend the nature and potential bias of algorithms fully. Chapter I already showed market automation is based on algorithms that do not take into account consumer meta-preferences.

Ignoring meta-preferences – which may be inaccessible to the algorithm- and instead focusing on the preferences suggested by previous consumer choices could reach an output/result that does not exactly predict plausible, meaning authentic and timely, consumer market choices. This potential 'deviation' between the consumer choice and the authentic preference is a circumstance that can hardly be demonstrated by the fundamental principle of protecting the freely given consent, both for the data-subject and the consumer entering a transaction.

Thus, the central problem is how to reach a fair outcome. Challenging conversations arise when a specific definition of fairness needs to be selected.

For instance, many fairness definitions compare the prediction of a decision process for different groups to the actual outcome. These group fairness measures can be simplified according to three main concepts of fair outcomes: independence, separation, and sufficiency.[87]

Against the background of diverse conceptual foundations of fairness, it isn't easy to specify precisely what the term means about AI. Some indication is to be found in the so-called Ethics Guidelines for Trustworthy artificial intelligence that have been published by the High-Level Expert Group on artificial intelligence,[88] an independent expert group that European Commission set up. The Guidelines count fairness among the 'four ethical principles, rooted in fundamental rights, which

opportunities' (2020) 62 Bus Inf Syst Eng 379-384; Alessandro Castelnovo, Riccardo Crupi, Greta Greco, Daniele Regoli, Ilaria Giuseppina Penco, Andrea Claudio Cosentini, 'A clarification of the nuances in the fairness metrics landscape' (2022) 12(1) Sci Rep 21.

[86] Solos Barocas, Moritz Hardt, Arvin Narayanan, *Fairness and machine learning* (MIT Press, 2018), available at <https://fairmlbook.org/> accessed 1 September 2023.

[87] ibid

[88] Commission, Ethics guidelines for trustworthy AI, 2018 <https://digitalstrategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> accessed 20 December 2022.

must be respected in order to ensure that AI systems are developed, deployed and used in a trustworthy manner'.[89]

However, for the fast development of data-driven technologies, concrete implementation instruments must be set up by joint initiatives involving lawyers, computer, neuroscientist, etc.

Authentic neuro-scientific interpretation of behaviours can help to get closer to the legal concept of fairness to the algorithmic implementation of fairness.

The exemplary field of robotics has already emerged where the governance of robotic issues is influenced by design and vice versa.[90]

As robot technology becomes more commonplace, design aspects will become increasingly important. In designs, engineers are required to work together with other scientists such as computer scientists and experts in human disciplines like ethicists, lawyers, and anthropologists. The need for integration between different disciplines expanded because it helps support holistic human-robot interaction design.

The design community has established many methods for engaging artefacts. It has branched out into subfields, such as interaction design and product design, which are highly relevant to the same human-robot interaction. Designers have unique opportunities to improve robotic products overall appeal and usefulness well beyond their technical functions and capabilities. The working method, essentially, aims to explore upcoming issues with a reciprocal exchange of information and

[89] Florian Möslein, Maximilian Horn 'Emerging rules on artificial intelligence: Trojan horses of ethics in the realm of law?' in Larry D. Di Matteo, André Janssen, Pietro Ortolani, Francisco de Elizalde, Michel Cannarsa, Mateja Durovic (eds) *The Cambridge handbook of lawyering in the digital age* (Cambridge University Press 2021) 77-95.

[90] Lars Erik Holmquist, Jodi Forlizzi, 'Introduction to Journal of Human-Robot Interaction Special Issue on Design' (2014) 3 J Hum Robot Interaction 1. A field where the concept of by-design developed was privacy. Privacy regulators in Canada, the US, and the EU have become increasingly vocal in calling for privacy to be designed-in to new products and services, rather than added as an afterthought following consumer complaints and regulatory action. Designed-in privacy is likely to be much more effective if included throughout the product or policy design lifecycle. A broader range of options is available to a designer than to an engineer trying to make changes to a product following a privacy incident. A privacy by design requirement is implied by Data Protection Directive Article 17. Parliament, Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Directive [1995] O.J L 281; see also Ian Brown, 'Britain's Smart Meter Programme: A Case Study in Privacy by Design' (2014) 28 Int'l Rev L Computers & Tech 172. The General Data Protection Regulation embraces privacy by design without detailing how it can, or should be applied.

advice. This will respond to the need to face complex issues undertaking opportune concrete actions, in design or manufacture. Not only do legal solutions require technologists' contribution to understanding complex technological applications, but also the scientific disciplines could reach appropriate findings and set up proper technological features based on the earlier involvement of social sciences.

4.3 The contribution of comparative methodology to think interdisciplinary when setting a legal design

The Proactive Law approach is based on a mix of methods to reach the desired objectives.

The integration of research approaches is needed to analyse the legal aspects of data-driven technologies.[91] Generally observing, in social sciences, it is commonly hoped that disciplinary barriers will be removed,[92] to set suitable goals.

Suppose there is no doubt in affirming the necessity to take an interdisciplinary approach to the regulation achievable by design. In that case, there is uncertainty about how to do it, and how to develop a suitable team working between stakeholders to realize it. All the previous considerations on algorithmic fairness testified it.

To identify the proper setting for the interdisciplinary work involving law,[93] a contribution can be given by legal comparison as a method.[94]

Notwithstanding the absence of an equal reciprocal exchange between law and other sciences due to limits commonly attributed to lawyers' attitude of approaching issues with very specific cultural baggage full of

[91] Michele Graziadei, 'Personal Autonomy and the Digital Revolution' in Alberto De Franceschi, Reiner Schulze (eds.), *Digital Revolution – New Challenges for Law* (Baden-Baden 2019) 16-17.

[92] Annelies Riles, 'Representing In-between: Law, Anthropology, and Rhetoric of Interdisciplinary' (1994) 3 University of Illinois Law Review 597; Mireille Hildebrandt, Jeanne Gaakeer, *Human Law and Computer Law: Comparative Perspectives* (Springer 2015).

[93] Nowadays, interdisciplinarity is extensively used in a non-technical way indicating, in practice, different approaches and degrees of interchange between law and other disciplines. Technically, the traditional literature categorized different levels of interaction: Basarab Nicolescu, 'Multidisciplinarity, Interdisciplinarity, Indisciplinarity, and Transdisciplinarity: Similarities and Differences' (2014) 2 RCC Perspectives 19-26.

[94] This comparative approach implies the necessity to consider law not as a field of law but a method of legal production. See Thomas Duve, 'European Legal History - Global Perspectives Working Paper for the Colloquium, European Normativity - Global Historical Perspectives' (Max-Planck-Institute for European Legal History 2013).

technical and domestic legal notions,[95] comparative law seems to be one of the most fruitful fields for experimenting with researches involving other sciences, because it is interdisciplinary by its very nature.[96]

Certainty, over the decades, different comparative law schools of thought have concretised the inherent interdisciplinarity of their field in different ways and with different degrees of integration of knowledge.[97] Nowadays, comparative law goes beyond doctrinal analyses that identify legal transplants or similarities and divergences between jurisdictions. It embraces the authentic meaning of those similarities and divergences, often discovering and emphasising their concrete roots that often have non-legal origins. Furthermore, to explore a legal issue or inquiry is not sufficient to investigate the content of legal rules, but also the implicit sources and values underpinned by it.[98] For this reason, Barbara Pasa and Gianni Sinni noted that:

'law and graphic communication design studies share the reflection on the relationship between alphabetical writing and visual codes in the formulation and communication of complex messages. While recognising the dominance of verbal language in human communication, at least in our cultural context, both law and graphic communication design specifically acknowledge that not all writing is alphabetical (such as in China) and that

[95] Vincenzo Zeno-Zencovich, *Comparative Legal Systems A Short Introduction* (RomaTrePress 2017) 97-99.

[96] Mary Ann Glendon, Paolo Carozza, Colin B. Picker, *Comparative legal tradition in a nutshell* (West Academic Publishing Co, 3d ed. 2008); Ugo Mattei, 'An Opportunity to be missed: the future of comparative law in the United States' (1998) 46 Am J Comp L 709; Uwe Kischel, *Comparative Law* (Oxford University Press 2019), Ch 1 B and 1 D; Nils Jansen, 'Comparative Law and Comparative Knowledge' in Mathias Reimann, Reinhard Zimmermann, *The Oxford Handbook of Comparative Law* (Oxford university Press 2019), 291-320. For an extensive lecture on comparison and its boundaries refer to Filippo Viglione, 'I «confini» nel diritto privato comparato' (2011) 3 La nuova giurisprudenza civile commentate 162-193.

[97] Comparatists have already complained about the positivistic approach of functionalism. See Gunter Frankenberg, *Comparative law as critique* (Edward Elgar 2016); Pierre Legrand, 'Negative Comparative Law' (2015) 10(2) Journal of Comparative Law 405-454; Pierre Legrand, Robert Munday (eds.), *Comparative Legal Studies: Traditions and Transitions* (Cambridge University Press 2003). To exemplify the explicit openness of comparative law to other non-legal knowledge, see Pier Giuseppe Monateri (ed.), *Methods of comparative law* (Edward Elgar 2013); Geoffrey Samuel, 'Does one need an understanding of methodology in law before one can understand methodology in comparative law?' in Mark Van Hoecke (ed.), *Methodologies of legal research: which kind of method for what kind of discipline?* (Hart Publishing 2014) 177-208.

[98] Pasa, Sinni (n 60).

not all writing is verbally oriented (such as the graphic symbols used to represent numbers'.[99]

A lot will depend on the research question and on researchers' ability to conduct a deep comparative analysis.[100] Scientific and technological subjects often require us to look at the phenomenon holistically.

The interdisciplinary perspective creates multiple methodological issues within comparative law. For example, the comparative lawyer needs to deal with linguistic specific terminology; integrate different research methods suitable for the different relevant disciplines – e.g. quantitative, qualitative- of data collection and analysis, and find standard objective parameters to evaluate findings and publications. This requires, on the one hand, clearly focused research aims and questions to ensure the feasibility of the project. On the other hand, the project should not be too abstract, narrow, or specialised to be meaningful beyond disciplinary borders. Comparative law studies can contribute to understanding the importance of deciding how to set up the research question to reach a suitable level of integration of knowledge.

The need for a preliminary understanding of the techno-scientific features means that lawyers need to be endowed with specific personal skills: the capacity to inquire, interact with, and understand different perspectives and adopt different methodological approaches and different ways of thinking.[101] These skills are often not facilitated in traditional Western legal education as it is settled in separate disciplines.[102]

Indeed, the recent interest in comparative law for empirical methodologies contributes to bridging the gap, offering suitable tools.[103]

[99] ibid

[100] For further constructive research elements: Roberto Scarciglia, *Metodi e comparazione giuridica* (2ª ed., Cedam 2018).

[101] Dario Antiseri, *I fondamenti epistemologici del lavoro interdisciplinare* (Armando editore 1972); Fabrizio Ravaglioli, 'Introduzione', in Fabrizio Ravaglioli (ed.), *Interdisciplinarietà* (Armando editore 1974) 71; Karl Larenz (ed.), *Storia del metodo nella scienza giuridica* (Giuffrè 1966). For an example of the use of numerical comparative law, see Mathias Siems, 'Comparative Legal Certainty: Legal Families and Forms of Measurement', in Mark Fenwick, Mathias Siems, Stefan Wrbkathe (ed.), *Shifting meaning of legal certainty in comparative and transnational law* (Hart Publishing 2017) 115.

[102] Giovanni Pascuzzi, 'La scienza giuridica è disciplinare: può esserlo la didattica nella facoltà di giurisprudenza?' (2007) V Il Foro Italiano 94.

[103] Francesco Parisi, Barbara Luppi, 'Quantitative Methods in Comparative Law', in Monateri (ed), *Methods* (n 97). Current developments in comparative law studies seek to develop a taxonomy of interdisciplinarity in response to modern research exigencies. Moreover, comparative lawyers recognise a new character of comparative law described as

The functional features of technological applications are only one of the fundamental aspects requiring a wider analysis perspective. The effect that new technologies have on society and the complex relationship between progress, law, and all the different factors influencing them – perceptions, economics – requires the comparative lawyer to be able to integrate knowledge that acts at different levels, such as epistemic, structural, and planning.

At this point, new technological challenges incentivise a new effort to reach authentic interdisciplinarity, distinguishing the level of interaction between disciplines by carefully pointing out the research question. The meaning attributed to interdisciplinary is evolving – even in the overseas context.[104] Posing the questions that need to be answered implies that a lawyer must have the ability to differentiate the several levels of integration between disciplines: with a basic level of interdisciplinarity, the same research question is settled up as traditional legal research, then considering other academic disciplines in order to answer it; with more advanced integration, research questions can be characterised by not only a legal nature, or incorporate quantitative and socio-legal methods into legal thinking; or combining the two interventions.[105]

One of the fascinating aspects at stake, when an interdisciplinary arena of stakeholders plans a legal design of a digital architecture is the need to analyse the deep mechanism of human nature and the functioning of the human mind. Following the observation expressed by the OECD with the

'implicit comparative law.' It aims to express the interconnection between the research of several comparative fields. It also opens the door to advance towards how to set up and formulate a research question, not purely legal. It encourages a change in methodology, incorporating new research methods into law – i.e. scientific methods. See Mathias Siems, *Comparative law* (Cambridge 2022) part II 'Extending the Methods of Comparative Law' (sections 8 and 9) 207-281. With specific regard to consumer law see Giesela Rühl, 'Behavioural analysis and comparative law: improving the empirical foundation for comparative legal research' in Hans-W. Micklitz, Anne-Lise Sibony, Fabrizio Esposito (eds.), *Research Methods in Consumer Law. A Handbook Handbooks of Research Methods in Law series* (EE Elgar 2018) 77-118.

[104] It is theorised that the importance of interdisciplinarity was first attributed to Roscoe Pound in 1907 and affirmed the importance for law professors to overcome the pure legal notions and to understand circumstances – such as social and economic conditions – where legal principles are applied. Roscoe Pound, 'The need for a sociological jurisprudence' (1907) 19 The Green Bag 5.

[105] Mathias Siems, 'The Taxonomy of Interdisciplinary Legal Research: Finding the Way Out of the Desert' (2009) 7 Journal of Commonwealth Law and Legal Education 5-17. The article proposes four different types of interdisciplinary legal research: one basic and three advanced types.

report on ‘consumer vulnerability in digital age’, ‘more evidence on consumer vulnerability is needed. Research has to date mainly focused on certain personal attributes and circumstances, such as age and income, rather than external conditions (e.g. digital market practices), individual states (e.g. emotions) and other attributes or circumstances (e.g. geographical remoteness). Traditional empirical methods, such as surveys, behavioural experiments, complaints analysis, focus groups and interviews, are promising avenues for capturing data on several less-researched factors. Though studying the temporal or contextual vulnerabilities peculiar to the digital environment, may require novel methods, e.g. involving studying ‘digital trace’ data or the outputs of businesses’ algorithms’.[106]

The contribution of cognitive psychology perfectly responds to what Raffaele Caterina noted in its article – ‘Comparative Law and the Cognitive Revolution’ – about the fact that the study of the mind could support the comparative study of law by posing new questions and challenging traditional approaches.[107] Due to the recognized importance of the ability to understand other people’s mental processes for human socialization, and to developing empathetic process[108], on one hand, and the importance of comparison to be based on collective knowledge, and sciences relate to human mind become mutual essential to formulate and investigate research questions on complex issue about human-computer interaction through digital architectures and designs.

[106] OECD (6 of the document).

[107] Raffaele Caterina, ‘Comparative Law and the Cognitive Revolution’ (2004) 78 Tul Law Rev 1501.

[108] Sofia Ranchordas discussed empathy is role in law and in digital times. See Sofia Ranchordas, ‘Empathy in digital administrative state’ (2022) 71 Duke Law Journal 1341.

Conclusions

This research has started from an explicit acknowledgement: in the digital market, it is a weak narrative to focus consumer autonomy exclusively on informed choice protection.

As suggested in Chapter I, adopting the fruitful Law 3.0 approach helps to understand why current policies and guidance reflect a shift towards user autonomy, which embraces a comprehensive vision of the interrelation between consumer and digital choice architectures, to result in ensuring qualitative information, as well as fair design patterns.

Data flows through spaces and across borders, regardless of boundaries. Irrespective of the fact that data evades borders, the law tries to pin it down in various ways and into specific legal policies. The dichotomy is captured by the tension between the formal current protection of consumer autonomy and its concrete efficacy that emerged from dark patterns. This study offers an overview of specific criticalities posed by the digital environment to the right of autonomy within a perspective of EU private law. It also aims to be a starting point for future trajectories in research.

With the persistent uncertainty surrounding the qualification of certain types of dark patterns used by businesses to exploit data, the goal of measuring the regulatory efficacy of autonomy protection becomes complex. The same data can offer different representations of facts, depending on how it is aggregated and matched.

Thus, a preliminary step of the analysis was the pragmatic understanding of the specificities of dark patterns in use and the variety of their purposes that, ultimately, impact on consumer choices. Their fast development and transformation process showed how data exploitation strategies can potentially prejudice autonomy, both through its technological infrastructure, and through how it communicates to the consumer. For this reason, digital consumer autonomy should currently receive protection from rules guaranteeing transparent communication, and from rules protecting fairness. Following this reasoning, Chapter II offered an overview of current regulation and recent case law.

This new 'combined' approach to autonomy requires enlarging the picture of regulatory regimes which serve the scope, considering consumer law, but also data protection law and competition law. If, on the one hand, this expansion gives a more comprehensive and realistic vision of the needed protection and coordination, enforcement problems increase too. Lastly, OECD suggested adequate enforcement actions, which have been implemented in response to regulatory gaps,[1] and novel methods (e.g. neurophysiological experiments to test vulnerabilities relating to specific cognitive burdens and difficulties).

From a more analytical point of view, this research reaches several findings. Design is crucial, but not everything. More evident is the changing nature of the concepts involved: the harms caused by dark patterns and the relevance of consumer bias to constrain his self-determination ultimately show a shift of impact from bilateral to 'ecosystem' transparency. Digital asymmetry interferes with the quality of information and the ability to process data.

In the era of Big Data and artificial intelligence, where aggregated data is used to learn about patterns and decision-making processes, the quality of input data and control of the training phase of algorithms seem to be of paramount importance. Poor data quality may lead to a breach of fundamental rights, undermining trust in the public authorities which use such applications.

Data-driven technologies can collect user data continuously, allowing choice architects to learn how different users interact in their *onlife*. The inferred behavioural patterns can be functional to transform the digital environment and to change, in turn, patterns of behaviour to secure suitable outcomes for the seller or platform. The interaction between consumer and market phenomena can exacerbate human cognitive bias and, consequently, his capacity for self-determination.

Furthermore, lawyers must consider the evolving conceptualization of traditional legal categories. For example, a new concept that adequately covers what is empirically discussed in legal and non-legal research, as 'digital vulnerability', could solve inquiries related to digital asymmetry

[1] OECD (digital Economic Papers), 'Consumer vulnerability in Digital Age' (June 23 2023) n. 355 available at: <https://www.oecd-ilibrary.org/science-and-technology/consumer-vulnerability-in-the-digital-age_4d013cc5-en> accessed 29 June 2023.

through competition regulation, considering the anti-competitive effects of dark patterns (see Chapter II).

All these findings align with the evolution courts in different jurisdictions, already attested: there is a need to individualize the 'shades' of traditional concepts to protect digital consumers. Consideration towards the notion of the average consumer in Chapter III testified to this need too.

Finally, insights for suitable legal models emerged from different perspectives. The kaleidoscopic concept of autonomy must be addressed broadly, through flexible standard to catch case-specific interpretations and assess specific and situational individual cognitive bias.

Consequently, thinking in more 'granular' terms – such as in terms of personalized law – could better respond to challenges derived from distinctive traits of threats to the fundamental right to autonomy. These emerging traits resulted in relativity, emphasized by the fact that a deceptive design can be tricky for one person and not for another, and transitoriness, proved by the fact that the same dark pattern can affect a person in one situation but not in different circumstances.

The number of jurisdictions taking a holistic approach to addressing digital consumer autonomy by strengthening data quality, data control, and designs across different policy areas is constantly increasing.

Similarly, the role of fundamental rights in the field of private law emphasised the extension of EU legislation to 'digital matters' and other new areas, not only for coherency but also, at the same time, to precisely define the relationship between fundamental rights and private law provisions, including the effects of enforcement. For example, DSA, analysed in the previous pages, plays a critical role in increasing transparency, fairness, and accountability with a comprehensive horizontal approach that counterbalances the challenges posed by the private actors' governance, such as online platforms.

To conclude, regulation by design becomes a functional and flexible approach to building constructive elements for a fair, lawful, and preventive form of data-subject/consumer autonomy protection. For example, implementing transparency by design is expected to contribute to fairness without interfering with the autonomy of market actors. Also, Chapter III exposed the proposal for future-proof development of digital fairness.

The need to reach a commonly accepted understanding of algorithm fairness emerged and testified to the still curvy and long way EU regulation must go to tackle the structural, technological challenges for autonomy.

The exigence to design effective digital architectures, which are complex by nature, cannot disregard the required dialogue between different stakeholders, even at a global level and with informal working tools: an essential exchange to step onto a new legal path toward the protection of a consolidated common core of digital consumer rights.

Vi aspettiamo su:

www.francoangeli.it

per scaricare (gratuitamente) i cataloghi delle nostre pubblicazioni

DIVISI PER ARGOMENTI E CENTINAIA DI VOCI: PER FACILITARE
LE VOSTRE RICERCHE.

Management
Finanza
Marketing
Operations
HR
Psicologia e psicoterapia: teorie e tecniche
Didattica, scienze della formazione
Economia, economia aziendale
Sociologia
Antropologia
Comunicazione e media
FrancoAngeli

Management, finanza, marketing, operations, HR
Psicologia e psicoterapia: teorie e tecniche
Didattica, scienze della formazione
Economia, economia aziendale
Sociologia
Antropologia
Comunicazione e media
Medicina, sanità

Architettura, design, territorio
Informatica, ingegneria
Scienze
Filosofia, letteratura, linguistica, storia
Politica, diritto
Psicologia, benessere, autoaiuto
Efficacia personale
Politiche e servizi sociali

Filosofia, letteratura, linguistica, storia
Politica,
Psicologia benessere, autoaiuto
Efficacia personale
Politiche e servizi sociali
FrancoAngeli

FrancoAngeli

La passione per le conoscenze

Redesigning Protection for Consumer Autonomy

European legal protection of consumer autonomy has been significantly changed in the digital environment, where algorithm-driven systems perform everything. This book focuses on protecting consumer autonomy facing the pervasive and global phenomenon of dark patterns: the expression includes various tactics that manipulate consumers by altering online choice architecture to thwart user preferences for objectionable ends. Overloading, skipping, stirring, hindering, and flicking are examples. Moving from the perspective that the sole traditional information approach is ineffective in protecting autonomy, the adopted methodology considers the multiple concerns revolving around the tight combination of transparent information and fair digital architectural design. Consequently, the comparative study of the new suitable regulatory directions arises across different legal fields, including data protection, consumer, and competition law. The relationship between deceptive designs, the nature of human-digital architecture interaction, and the techno-legal paradigms emphasises which future changes in European private law could integrate legal rules into fair designs to protect digital consumer autonomy effectively. Specific importance will be attributed to the functionality of comparative methodology to include non-legal essential insights (e.g. behavioural, informatic elements) into pragmatic and global regulatory paths and models.

Giorgia Guerra, Ph.D., Trento University; post-doc, Padua University. She is an Assistant Professor in comparative private law at the Department of Law of the University of Verona, where she teaches comparative legal systems and comparative and transnational law and technology (data science master). She has an extensive publications track. In 2018 she published *La sicurezza dei prodotti robotici in prospettiva comparatistica. Dal cambiamento tecnologico all'adattamento giuridico* (il Mulino). She has held the National qualification (Habilitation) to second-level professor (associate) since August 2021.

FrancoAngeli
La passione per le conoscenze